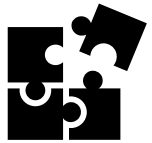
Cybersicherheit bei überwachungs-bedürftigen Anlagen

Workshop

Mehr Wert.
Mehr Vertrauen.

Unsere Agenda

Wichtige Begriffe und Grundlagen → Die TRBS 1115-1 → Umsetzung der Cybersecurity → Prüfung durch die ZÜS



Unsere Agenda

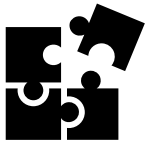
§

Wichtige Begriffe und Grundlagen

Die TRBS 1115-1

Umsetzung der Cybersecurity

Prüfung durch die ZÜS



Wichtige Begriffe

Cyber-Security

Risiko

ZÜS

Angriffswege

Gefährdung

TRBS vs. EmpfBS

Gefährdungsbeurteilung

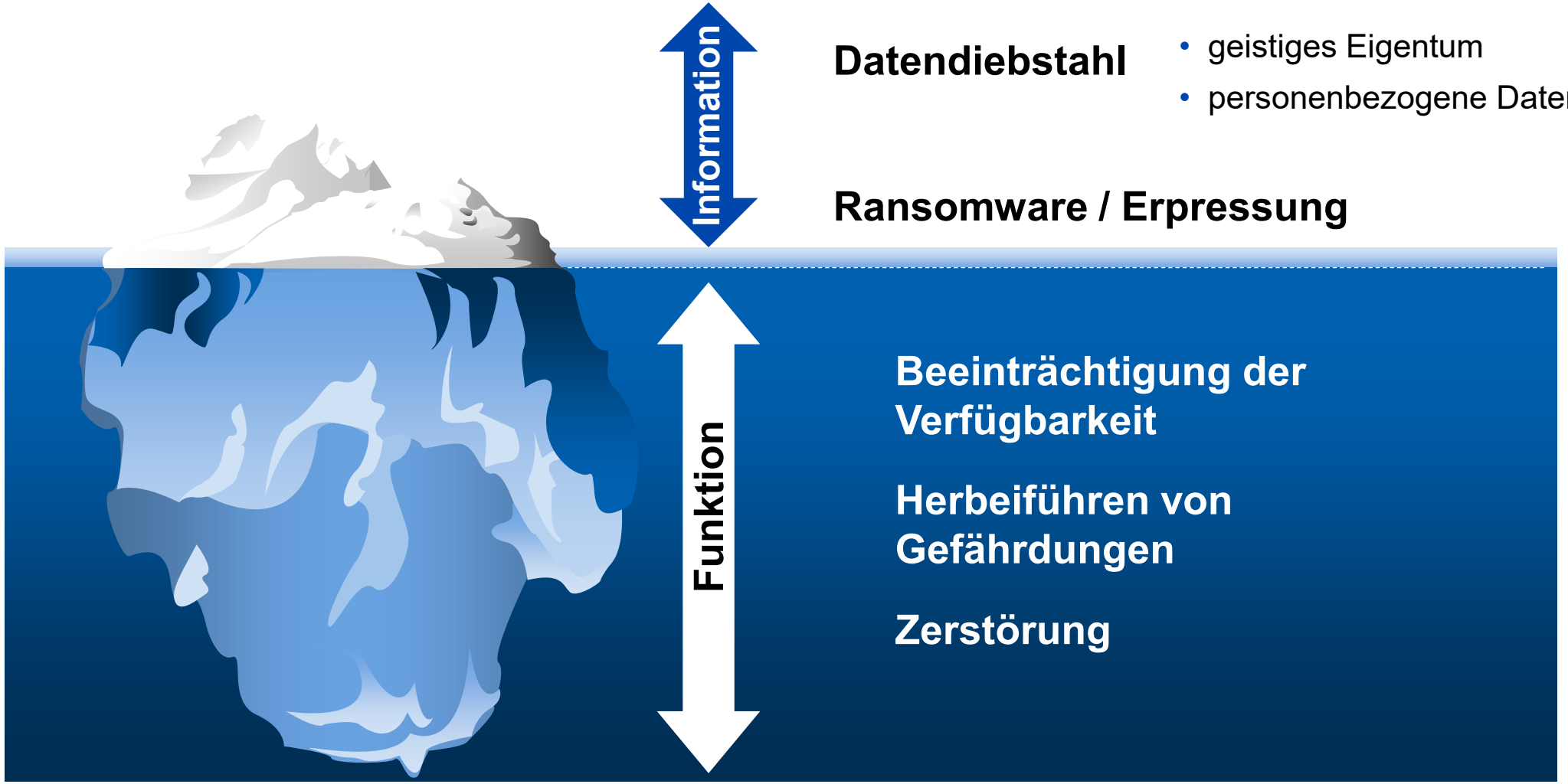
Schutzziel

OT

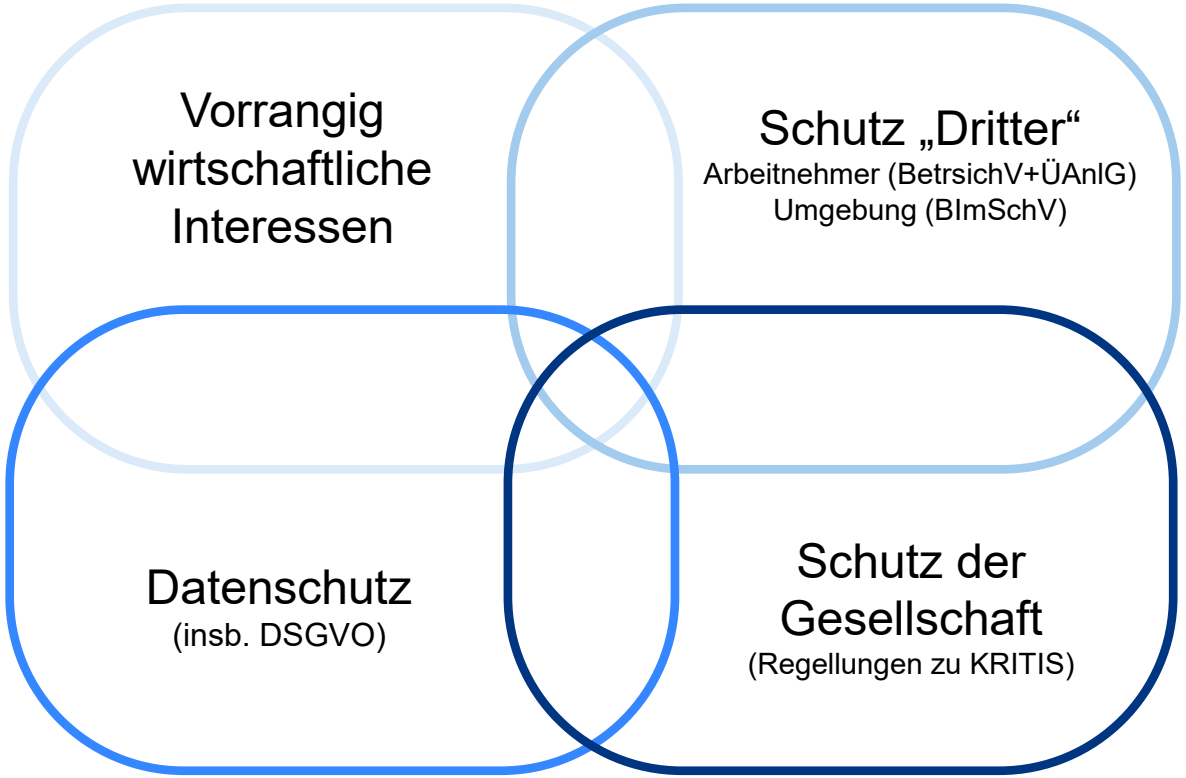
EK-ZÜS

Tätermodelle

Informationen oder Funktionen



Schutzziele

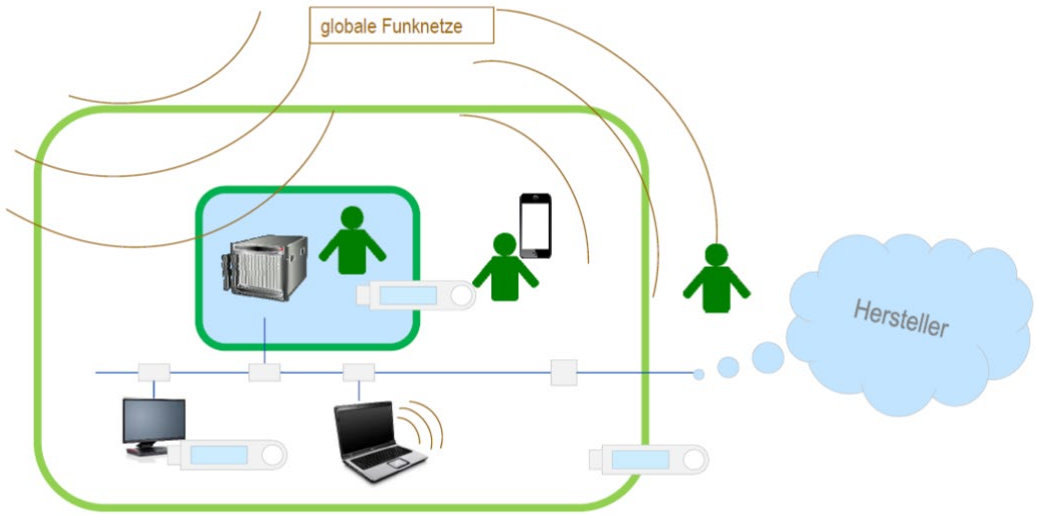


Die **Schutzziele** bestimmen die **schutzbedürftigen Systeme** und ihren **Schutzbedarf**

Frage: Welche Wege eines Cyberangriffs können Sie sich vorstellen?

Woher wissen Sie, dass Sie an alles gedacht haben?

Wege eines Angriffs



Bundesamt für Sicherheit in der Informationstechnik

Industrial Control System Security

Top 10 threats and countermeasures 2022

Top 10 Threats	Trend since 2019
Infiltration of malware via removable media and mobile systems	→
Infection with malware via Internet and Intranet	↑
Human error and sabotage	→
Compromise of extranet and cloud components	↗
Social engineering and phishing	→
(D)DoS attacks	→
Internet-connected control components	↗
Intrusion via remote maintenance access	↗
Technical failure and force majeure	→
Soft- and hardware vulnerabilities in the supply chain	↑

https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005E.pdf

Unsere Agenda

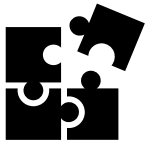
§

Wichtige Begriffe und Grundlagen

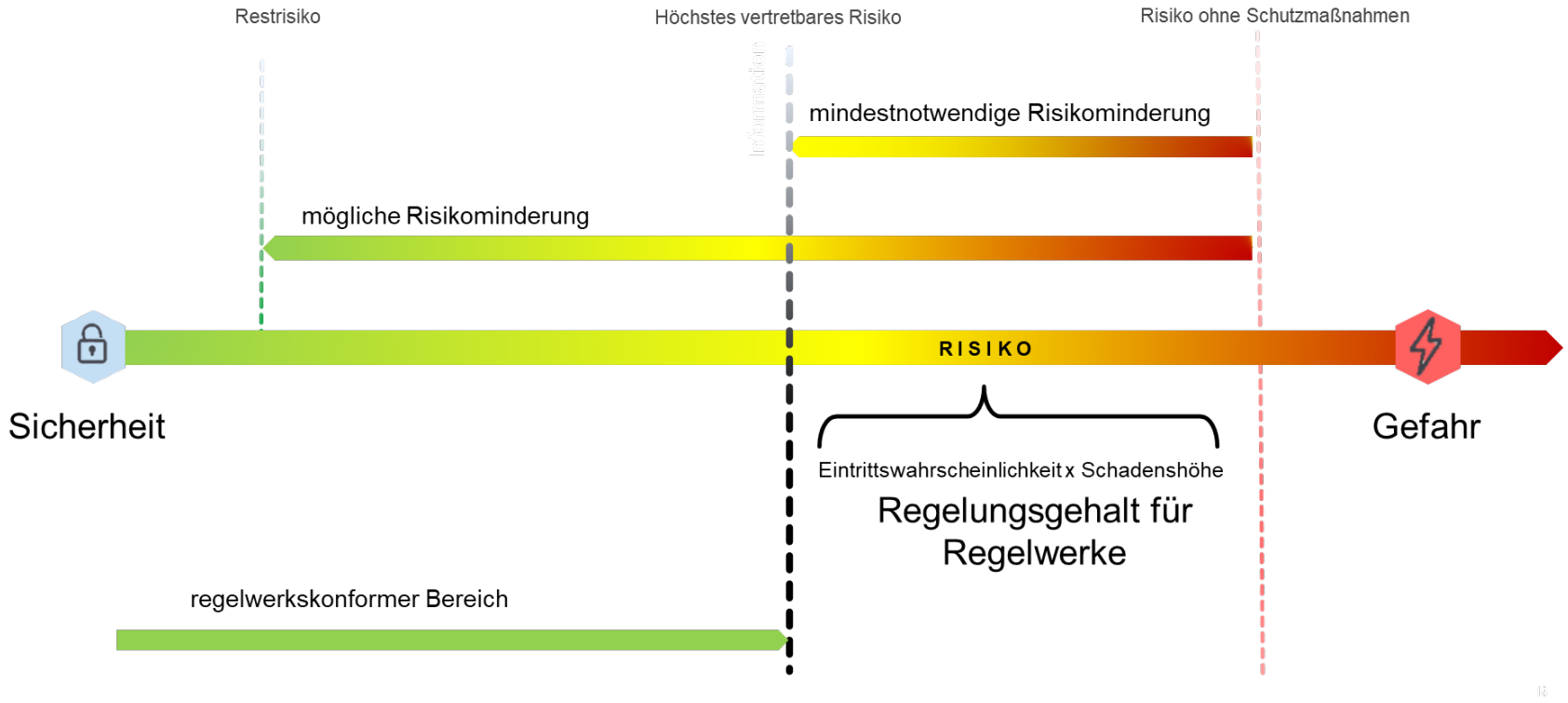
Die TRBS 1115-1

Umsetzung der Cybersecurity

Prüfung durch die ZÜS

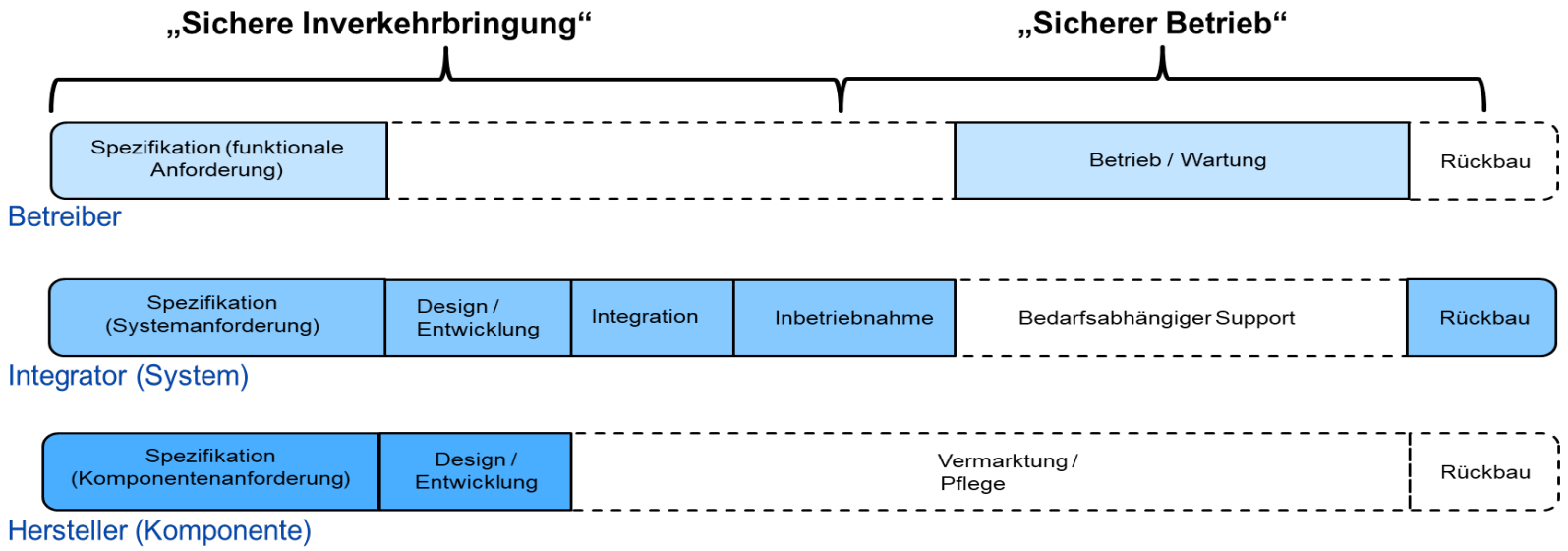


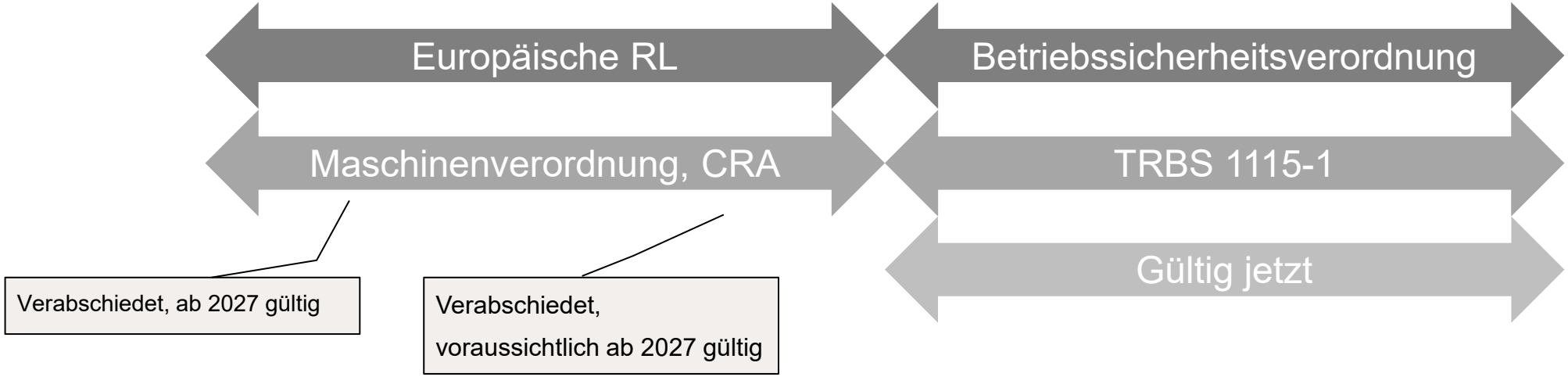
Ab wann wird die Sicherheit reguliert?



Cyberangriffe werden zunehmend als erwartbar angesehen.
Sicherheit bedeutet in diesem Fall, die erforderliche Safety und Security sicherzustellen!

Was macht die Produktsicherheit?





Relevante Vorgaben

(Pflichten des Arbeitgebers § 4 der BetrSichV)
Arbeitsmittel dürfen erst verwendet werden, ….

TRBS 1115-1 „..Cyber-Sicherheit für sicherheitsrelevante MSR-Einrichtungen“

Cyberbedrohungen können dazu führen, dass eine sicherheitsrelevante MSR-Einrichtung ihre Sicherheitsfunktion nicht mehr ausüben kann oder sogar zusätzliche Gefährdungen herbeigeführt werden.

(2) Diese TRBS beschreibt ergänzend zu TRBS 1201 auch die Durchführung von Prüfungen zur Cybersicherheit sowie das Vorgehen bei Änderungen von Arbeitsmitteln in Zusammenhang mit der Cybersicherheit von sicherheitsrelevanten MSR-Einrichtungen.

ÜAnlG § 7
Prüfung von üA

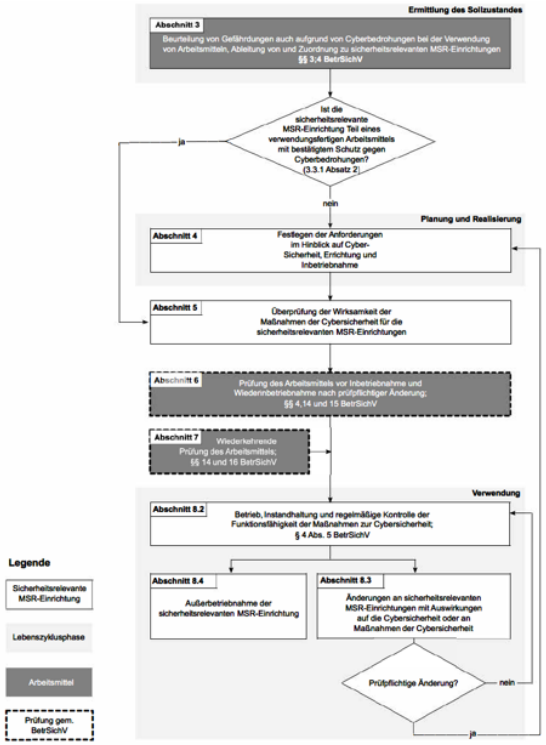
Der Betreiber einer überwachungsbedürftigen Anlage hat sicherzustellen, dass die Anlage auf ihren sicheren und ordnungsgemäßen Zustand geprüft wird.

BetrSichV:Anhang 2
Prüfvorschriften für ZÜS

Die Prüfungen sind mit dem Ziel durchzuführen, den sicheren Betrieb der ……(üA) bis zur nächsten Prüfung zu gewährleisten.

TRBS 1115-1 und TRBS 1115

Sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen



Technische Regel für Betriebssicherheit | Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen | TRBS 1115-1

Die Technischen Regeln für Betriebssicherheit (TRBS) geben den Stand der Technik, Arbeitsmedizin und Arbeitshygiene sowie sonstige gesicherte arbeitswissenschaftliche Erkenntnisse für die Verwendung von Arbeitsmitteln wieder.

Sie werden vom

Ausschuss für Betriebssicherheit

ermittelt bzw. angepasst und vom Bundesministerium für Arbeit und Soziales (BMAS) im Gemeinsamen Ministerialblatt (GMBl) bekannt gegeben.

Die TRBS 1115-1 konkretisiert im Rahmen ihres Anwendungsbereichs die Anforderungen der Betriebssicherheitsverordnung. Bei Einhaltung dieser Technischen Regeln kann der Arbeitgeber davon ausgehen, dass die entsprechenden Anforderungen der Verordnung erfüllt sind. Wählt der Arbeitgeber eine andere Lösung, muss er damit mindestens die gleiche Sicherheit und den gleichen Gesundheitsschutz für die Beschäftigten erreichen.

Inhalt

1 Anwendungsbereich
2 Begriffsbestimmungen
3 Anforderungen der Cybersicherheit an sicherheitsrelevante MSR-Einrichtungen
4 Planung und Realisierung der Ausrüstung eines Arbeitsmittels mit einer sicherheitsrelevanten MSR-Einrichtung durch den Arbeitgeber im Hinblick auf Cybersicherheit
5 Überprüfung der Wirksamkeit der Cybersicherheitsmaßnahmen
6 Prüfung des Arbeitsmittels vor Inbetriebnahme und Wiederinbetriebnahme nach prüfpflichtiger Änderung nach §§ 14 und 15 BetrSichV
7 Wiederkehrende Prüfung von Arbeitsmitteln mit sicherheitsrelevanten MSR-Einrichtungen nach §§ 14 und 16 BetrSichV
8 Verwendung und Instandhaltung
Anhang 1 Management der Cybersicherheit
Anhang 2 Regelwerke und Normen

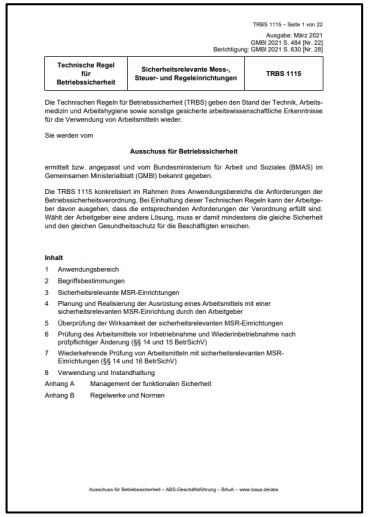
1 Anwendungsbereich

(1) Diese Technische Regel konkretisiert die Betriebssicherheitsverordnung (BetrSichV) im Hinblick auf die Ermittlung und Festlegung erforderlicher Cybersicherheitsmaßnahmen für die dauerhafte Sicherstellung der Funktionsfähigkeit von sicherheitsrelevanten Mess-, Steuer- und Regeleinrichtungen (MSR-Einrichtungen), die als technische Schutzmaßnahme für die sichere Verwendung eines Arbeitsmittels inklusive einer überwachungsbedürftigen Anlage eingesetzt werden.

Cyberbedrohungen können dazu führen, dass eine sicherheitsrelevante MSR-Einrichtung ihre Sicherheitsfunktion nicht mehr ausüben kann oder sogar zusätzliche Gefährdungen herbeigeführt werden.

TRBS 1115-1
Cybersicherheit

TRBS 1115
Funktionale Sicherheit



Technische Regel für Betriebssicherheit | Sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen | TRBS 1115

Die Technischen Regeln für Betriebssicherheit (TRBS) geben den Stand der Technik, Arbeitsmedizin und Arbeitshygiene sowie sonstige gesicherte arbeitswissenschaftliche Erkenntnisse für die Verwendung von Arbeitsmitteln wieder.

Sie werden vom

Ausschuss für Betriebssicherheit

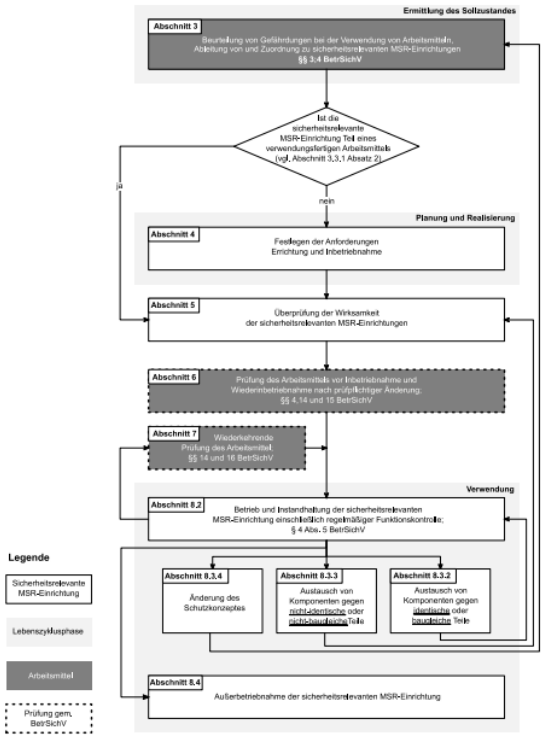
ermittelt bzw. angepasst und vom Bundesministerium für Arbeit und Soziales (BMAS) im Gemeinsamen Ministerialblatt (GMBl) bekannt gegeben.

Die TRBS 1115 konkretisiert im Rahmen ihres Anwendungsbereichs die Anforderungen der Betriebssicherheitsverordnung. Bei Einhaltung dieser Technischen Regeln kann der Arbeitgeber davon ausgehen, dass die entsprechenden Anforderungen der Verordnung erfüllt sind. Wählt der Arbeitgeber eine andere Lösung, muss er damit mindestens die gleiche Sicherheit und den gleichen Gesundheitsschutz für die Beschäftigten erreichen.

Inhalt

1 Anwendungsbereich
2 Begriffsbestimmungen
3 Sicherheitsrelevante MSR-Einrichtungen
4 Planung und Realisierung der Ausrüstung eines Arbeitsmittels mit einer sicherheitsrelevanten MSR-Einrichtung durch den Arbeitgeber
5 Überprüfung der Wirksamkeit der sicherheitsrelevanten MSR-Einrichtungen
6 Prüfung des Arbeitsmittels vor Inbetriebnahme und Wiederinbetriebnahme nach prüfpflichtiger Änderung (§§ 14 und 15 BetrSichV)
7 Wiederkehrende Prüfung von Arbeitsmitteln mit sicherheitsrelevanten MSR-Einrichtungen (§§ 14 und 16 BetrSichV)
8 Verwendung und Instandhaltung
Anhang A Management der funktionalen Sicherheit
Anhang B Regelwerke und Normen

Gemeinsames Ziel ist die Zuverlässigkeit sicherheitsrelevanter Systeme



TRBS 1115-1

TRBS 1115 Teil 1 – Seite 1 von 20

Ausgabe: November 2022
GMBl 2023 S. 522 [Nr. 25]

Technische Regel für Betriebssicherheit	Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen	TRBS 1115 Teil 1

Die Technischen Regeln für Betriebssicherheit (TRBS) geben den Stand der Technik, Arbeitsmedizin und Arbeitshygiene sowie sonstige gesicherte arbeitswissenschaftliche Erkenntnisse für die Verwendung von Arbeitsmitteln wieder.

Sie werden vom **Ausschuss für Betriebssicherheit** ermittelt bzw. angepasst und vom Bundesministerium für Arbeit und Soziales (BMAS) im Gemeinsamen Ministerialblatt (GMBl) bekannt gegeben.

Die TRBS 1115 Teil 1 konkretisiert im Rahmen ihres Anwendungsbereichs Anforderungen der Betriebssicherheitsverordnung. Bei Einhaltung dieser Technischen Regeln kann der Arbeitgeber davon ausgehen, dass die entsprechenden Anforderungen der Verordnung erfüllt sind. Wählt der Arbeitgeber eine andere Lösung, muss er damit mindestens die gleiche Sicherheit und den gleichen Gesundheitsschutz für die Beschäftigten erreichen.

1 Anwendungsbereich

2 Begriffsbestimmungen

3 Anforderungen der Cybersicherheit an sicherheitsrelevante MSR-Einrichtungen

4 Planung und Realisierung der Ausrüstung eines Arbeitsmittels mit einer sicherheitsrelevanten MSR-Einrichtung im Hinblick auf Cybersicherheit durch den Arbeitgeber

5 Überprüfung der Wirksamkeit der Cybersicherheitsmaßnahmen

6 Prüfung des Arbeitsmittels vor Inbetriebnahme und Wiederinbetriebnahme nach prüfpflichtiger Änderung nach §§ 14 und 15 BetrSichV

7 Wiederkehrende Prüfung von Arbeitsmitteln mit sicherheitsrelevanten MSR-Einrichtungen nach §§ 14 und 16 BetrSichV

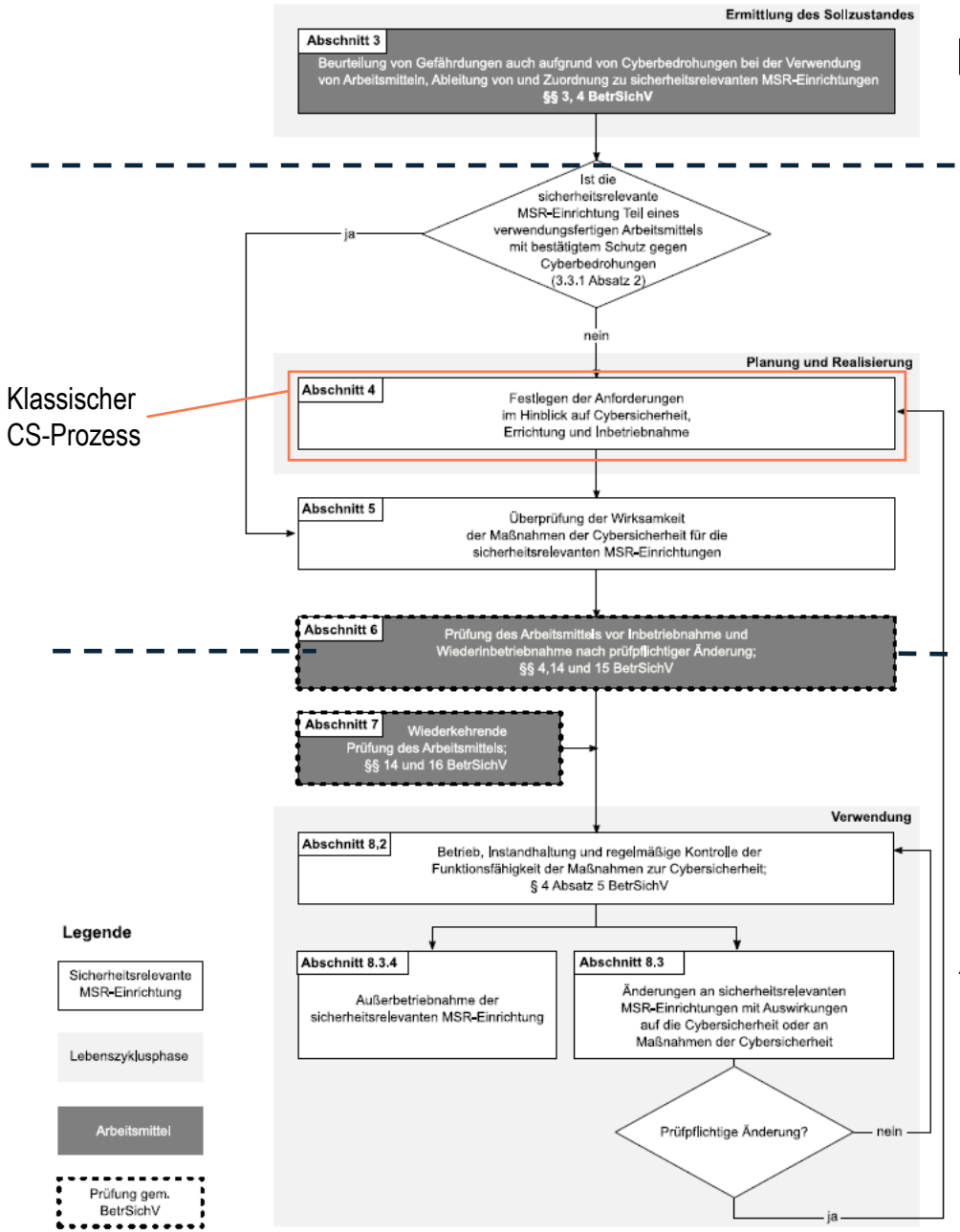
8 Verwendung und Instandhaltung

Anhang 1

Management der Cybersicherheit

Anhang 2

Regelwerke und Normen



Konzeption

Was brauche ich grundsätzlich?

Realisierung

Was verwende ich?
Ist das geeignet?
Funktioniert es wie geplant?

Betrieb

Was muss ich tun, damit die Anlage sicher bleibt?

Welche Teile der Anlage sind nicht betroffen?

Ausgabe: November 2022
GMBl 2023 S. 522 [Nr. 25]

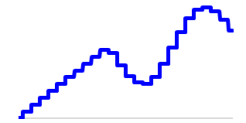
Technische Regel für Betriebssicherheit	Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen	TRBS 1115 Teil 1

1 Anwendungsbereich

(4) Diese TRBS behandelt keine Arbeitsmittel oder sicherheitsrelevanten MSR-Einrichtungen, die aufgrund nicht vorhandener Schnittstellen (sowohl kabelgebunden als auch kabellos) nicht kompromittiert werden können.

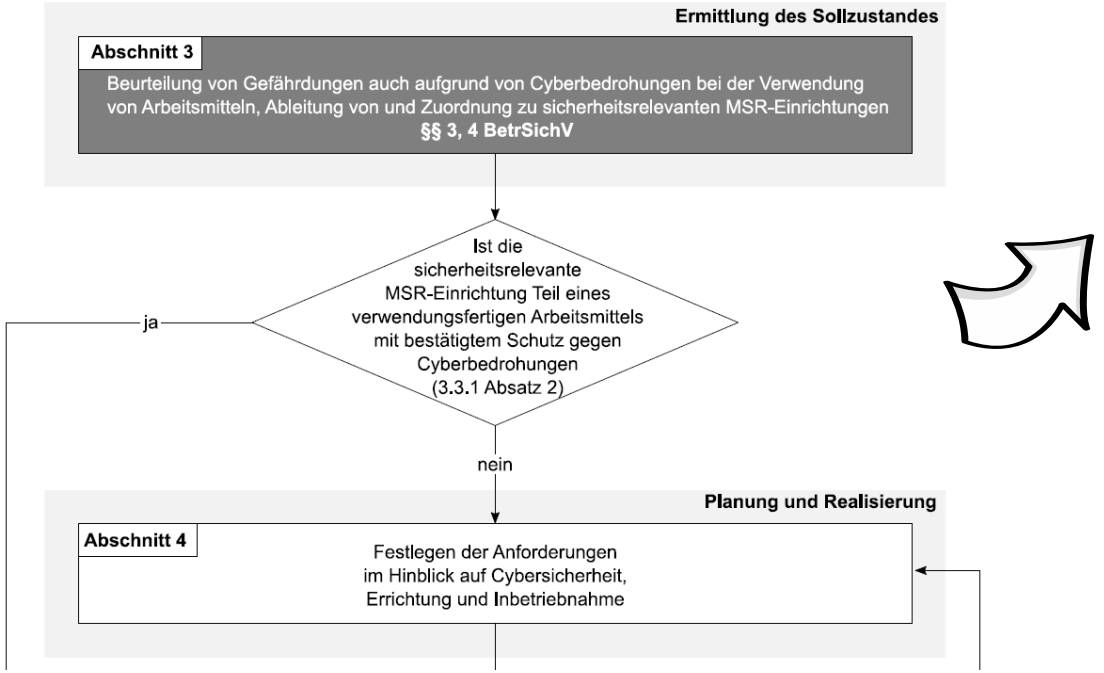
(5) Diese TBRS betrachtet nicht die Abwehr von wirtschaftlichen Schäden oder von Angriffen auf den Datenschutz (z. B. von personenbezogenen Daten). Sie kann dafür gleichwohl als Erkenntnisquelle herangezogen werden.

Schnittstellen meint digitale Schnittstellen

Analoge Informationen Beispiel: Schallplatte	
Binäre Informationen Beispiel: Lichtschalter (wertdiskret)	
Digitale Informationen Beispiel: MP3 (wert- und zeitdiskret)	

Schnittstellen zur Übergabe komplexer Informationen zwischen softwarebasierten Systemen

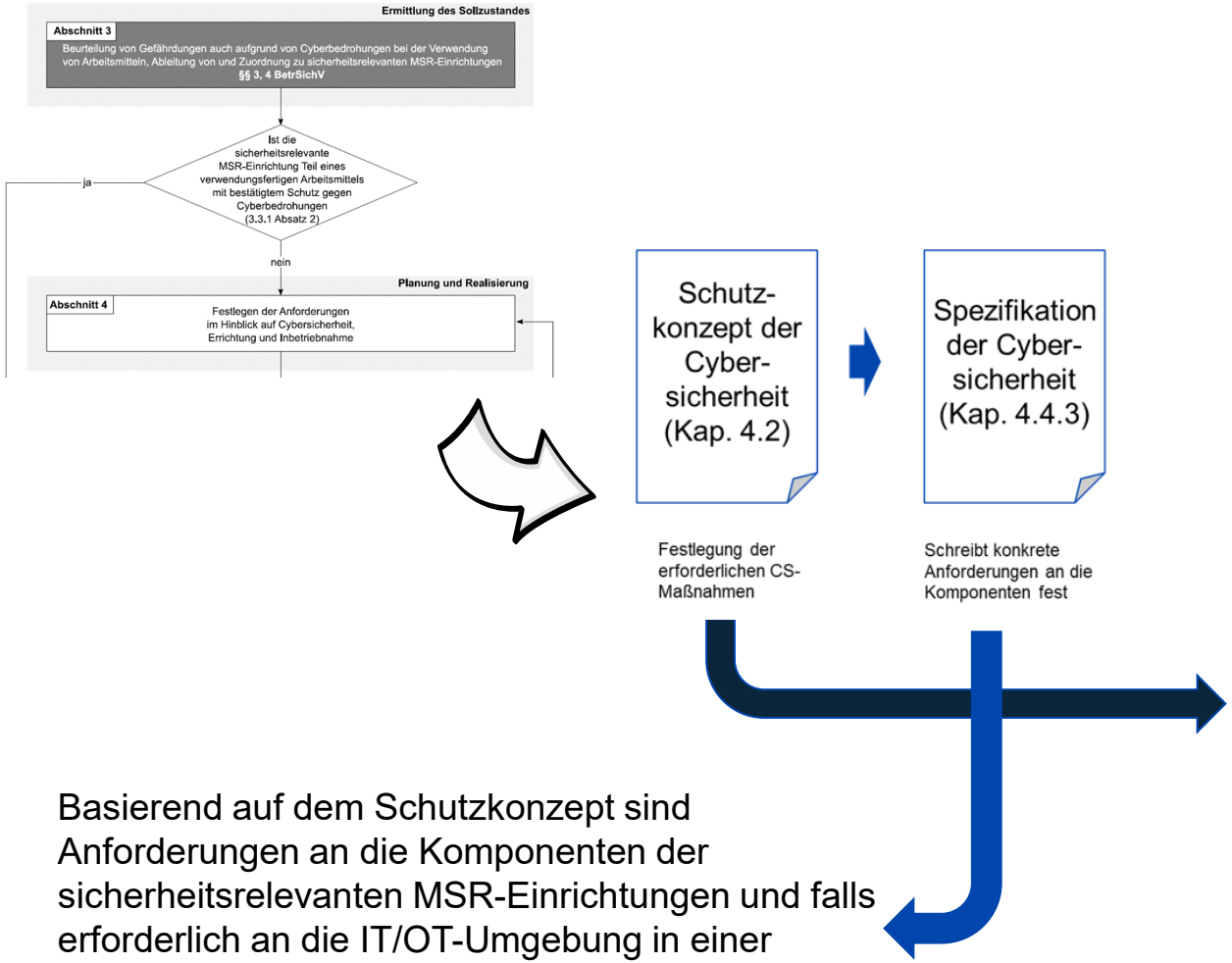
TRBS 1115-1



Die sicherheitsrelevante MSR-Einrichtung wird als Teil eines verwendungsfertigen Arbeitsmittels durch den Hersteller des Arbeitsmittels auf dem Markt bereitgestellt, wobei ein anforderungsgerechter Schutz gegen Cyberbedrohungen nach dem Stand der Technik bestätigt wurde.

1. Kann man sinngemäß auch anwenden, wenn die komplette MSR-Einrichtung verwendungsfertig bereitgestellt wurde
2. Kann nicht angewendet werden, wenn nur einzelne Komponenten Teil der Bestätigung sind
3. Der Prozess des Herstellers gleicht weitestgehend dem des Betreibers
4. Die Belastbarkeit der Bestätigung muss belegbar sein (z.B. anerkannte Zertifizierung oder geeignete Dokumentation)

Vorgehen der TRBS 1115-1

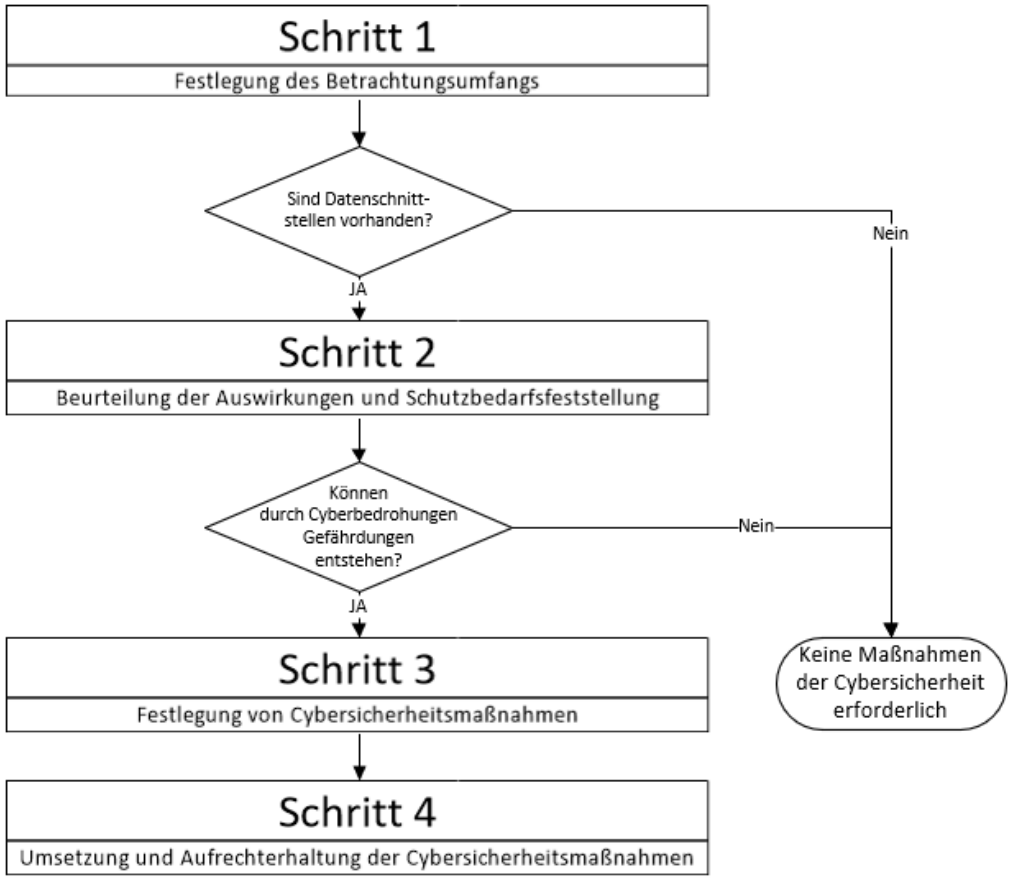


Basierend auf dem Schutzkonzept sind Anforderungen an die Komponenten der sicherheitsrelevanten MSR-Einrichtungen und falls erforderlich an die IT/OT-Umgebung in einer Spezifikation der Cybersicherheit festzulegen.

1. **Erfassung aller Elemente** gemäß Abschnitt 3.2 der **sicherheitsrelevanten MSR-Einrichtungen** und **der IT/OT-Umgebung** im erforderlichen Umfang. *„Asset-Erfassung“*
2. **Erfassung und Bewertung von Bedrohungen** der Integrität und Verfügbarkeit der sicherheitsrelevanten MSR-Einrichtungen, die durch Cyberbedrohung dieser Elemente ausgehen. *„Bedrohungsanalyse“*
3. **Auswahl und Umsetzung von Cybersicherheits-maßnahmen**, um den Cyberbedrohungen in geeigneter Weise zu begegnen und die Auswirkungen im erforderlichen Umfang zu begrenzen. (…) Auf die **erforderliche Rückwirkungsfreiheit** der Cybersicherheitsmaßnahmen auf die Sicherheitsfunktion ist zu achten. *„Maßnahmen“*
4. Festlegungen der **Fristen oder Anlässe** für die Durchführung **von Aktualisierungen und Kontrollen**. *„Aktualisierungen und Kontrollen“*
5. **Festlegung** eines Vorgehens zur **regelmäßigen Ermittlung von Schwachstellen** in der IT/OT-Umgebung und den Cyberbedrohungen. *„kontinuierliche Schwachstellenanalyse“*

Vorgehen der TRBS 1115-1

1. **Erfassung aller Elemente** gemäß Abschnitt 3.2 der **sicherheitsrelevanten MSR-Einrichtungen** und **der IT/OT-Umgebung** im erforderlichen Umfang. *„Asset-Erfassung“*
2. **Erfassung und Bewertung von Bedrohungen** der Integrität und Verfügbarkeit der sicherheitsrelevanten MSR-Einrichtungen, die durch Cyberbedrohung dieser Elemente ausgehen. *„Bedrohungsanalyse“*
3. **Auswahl und Umsetzung von Cybersicherheits-maßnahmen**, um den Cyberbedrohungen in geeigneter Weise zu begegnen und die Auswirkungen im erforderlichen Umfang zu begrenzen. … Auf die **erforderliche Rückwirkungsfreiheit** der Cybersicherheitsmaßnahmen auf die Sicherheitsfunktion ist zu achten. *„Maßnahmen“*
4. Festlegungen der **Fristen oder Anlässe** für die Durchführung **von Aktualisierungen und Kontrollen**. *„Aktualisierungen und Kontrollen“*
5. **Festlegung** eines Vorgehens zur **regelmäßigen Ermittlung von Schwachstellen** in der IT/OT-Umgebung und den Cyberbedrohungen. *„kontinuierliche Schwachstellenanalyse“*



Gibt es konkrete Fragen zur TRBS 1115-1?

Unsere Agenda

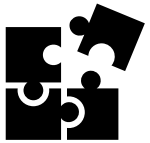
§

Wichtige Begriffe und Grundlagen

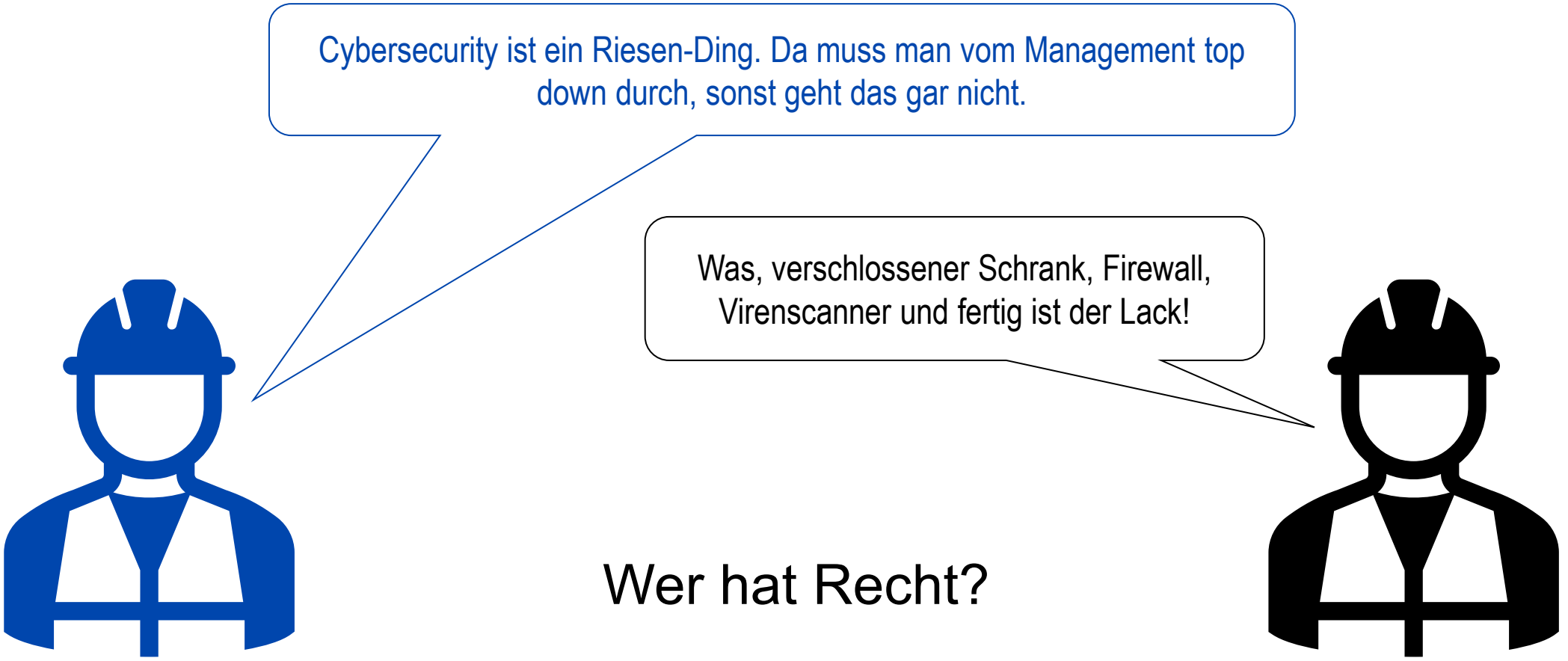
Die TRBS 1115-1

Umsetzung der Cybersecurity

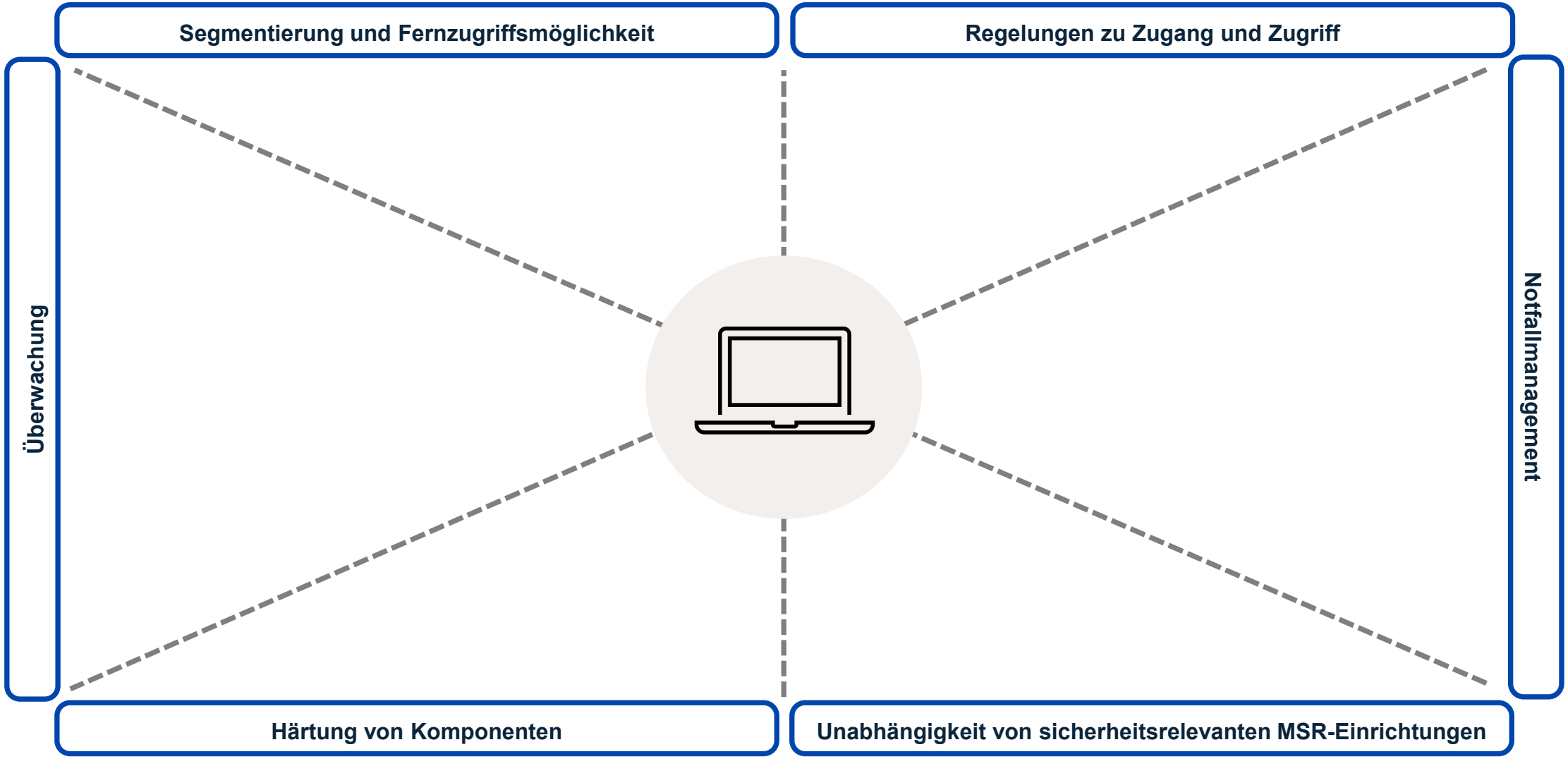
Prüfung durch die ZÜS



Cybersecurity, Hype oder Fail?

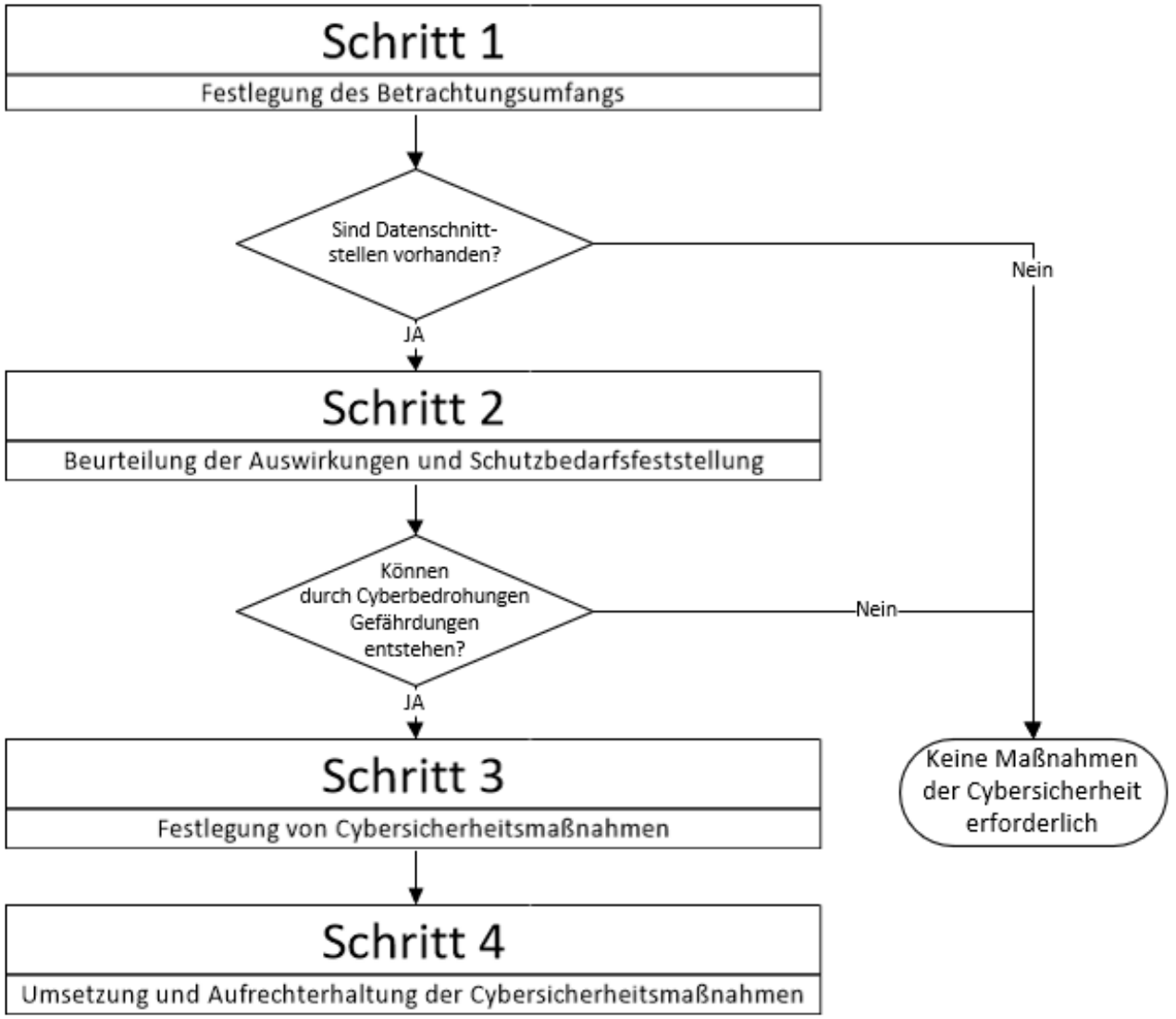


Was für Cybersicherheitsmaßnahmen gibt es?

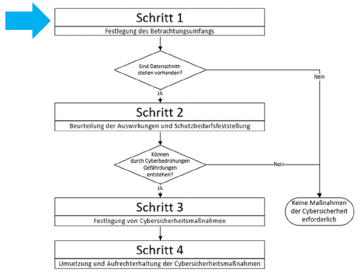


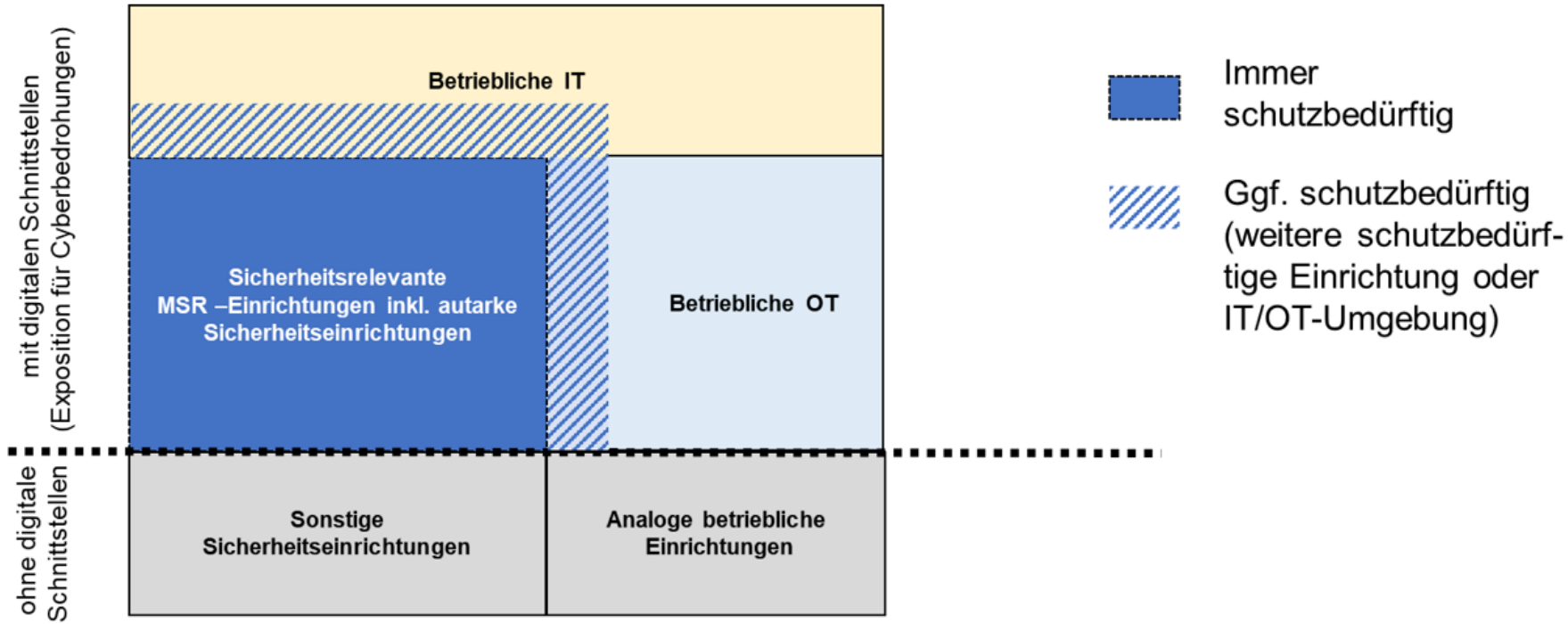
Sortierung gemäß TRBS 1115-1

Arbeitshilfe TÜV SÜD



Schritt 1: Festlegung des Betrachtungsumfangs

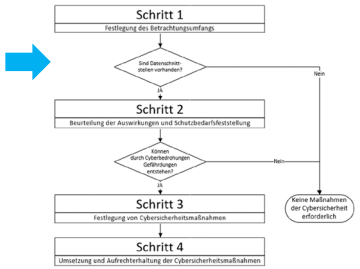




aus EK ZÜS-Beschluss B-002

+ Erfassung der Informationen entsprechend TRBS 1115-1 Abschnitt 3.2 zu den schutzbedürftigen Systemen

Entscheidungspunkt 1, Schnittstellen ja oder nein



Kabelgebunden

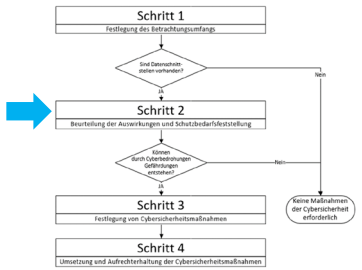
- RJ45 Netzwerkstecker (TCP/IP)
- RJ11 Telefonstecker
- D-SUB (RS232 / RS485)
- USB
- SD-Karte
- Herstellereigene Steckverbinder
- HART
- Kabeleinführung mit Klemmen

Funkverbindung

- Mobilfunk (2G/4G/5G)
- Bluetooth
- WiFi (W-LAN)
- NFC (Nahfeldkommunikation)
- ZigBee (Spezialnetzwerk)

Frage: Was machen wir mit einer Mensch-Maschine-Schnittstelle?

Schritt 2: Beurteilung der Auswirkungen und Schutzbedarfsfeststellung



1

Schutzbedürftig, Ja oder nein

Variante 1: überobligatorische Festschreibung als schutzbedürftiges System

Variante 2: einfache Kontrollfragen (z.B.)

Was passiert bei einer Fehlauslösung?
Was passiert bei einer Blockierung?
Was passiert bei einer Parameter- oder Funktionsänderung

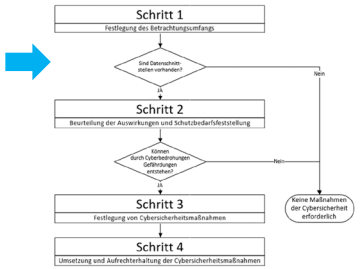
Variante 3: komplexe Analyse (insbesondere bei zusammen wirkenden Systemen erforderlich

2

Differenzierung des Schutzbedarfs erwünscht?

Möglich, oft sinnvoll, aber nicht zwingend

Entscheidungspunkt 2, Gefährdung ja oder nein



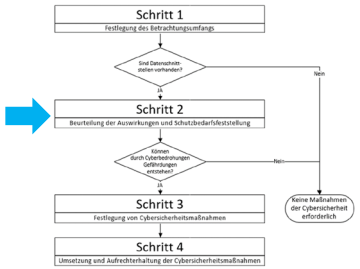
Ausgabe: März 2018
GMBl 2018 S. 401 [Nr. 22]
Änderungen und Ergänzungen: GMBl 2019 S. 292 [Nr. 13-16]

Technische Regeln für Betriebssicherheit	**Gefährdungsbeurteilung**	**TRBS 1111**

(2) **Gefährdung** ist die Möglichkeit eines Gesundheitsschadens oder einer gesundheitlichen Beeinträchtigung ohne bestimmte Anforderungen an deren Ausmaß oder Eintrittswahrscheinlichkeit.

Bei Unklarheit sollte man sich die Frage stellen, ob das etablierte Regelwerk der Safety bereits Schutzmaßnahmen vorsieht

Schritt 3:Festlegung von Cybersicherheitsmaßnahmen



Management
z.B. ISO 27001

Übergeordnete Themenkomplexe für Maßnahmen
z.B. Foundational Requirements IEC 62443

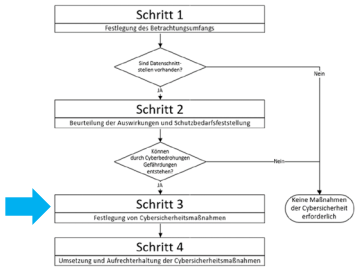
Technische CS-Maßnahmen

Organisatorische Maßnahmen

Allgemeine Vorgaben der TRBS-1115-1 Ab. 4.5 als Orientierung verwenden

Keine konkreten Vorgaben für anzuwendende Regelwerke oder qualitative Anforderungen in der TRBS 1115-1 enthalten

Schritt 3:Festlegung von Cybersicherheitsmaßnahmen



4.5 Cybersicherheitsmaßnahmen

4.5.1 Auslegungsgrundsätze

(1) Zum Schutz vor Cyberbedrohungen sind die Schnittstellen von sicherheitsrelevanten MSR-Einrichtungen, der Vernetzungsgrad und die Zugriffsmöglichkeiten auf das für die Verwendung des Arbeitsmittels notwendige Maß zu reduzieren.

(2) Zusätzlich ist auf die ausreichende Widerstandsfähigkeit der betroffenen technischen Systeme der sicherheitsrelevanten MSR-Einrichtung selbst und der IT/OT-Umgebung gegenüber Cyberbedrohungen zu achten.

(3) Methoden und Verfahren sind so festzulegen, dass auch ergonomische Aspekte sowie ihre Akzeptanz bei den Beschäftigten berücksichtigt werden, damit eine Maßnahme der Cybersicherheit keine unsicheren Verhaltensweisen begünstigt (z. B. längere Wechselintervalle und starke Passwörter oder Einsatz von Token anstatt häufige Passwortwechsel).

➔ „Minimalitätsprinzip“

➔ Resilience der S-MSR und IT- / OT-Umgebung

➔ Akzeptanz bei den Beschäftigten

Schritt 3:Cybersicherheitsmaßnahmen nach 4.5.2 (2)

Segmentierung und Fernzugriffsmöglichkeit
- Netzwerkseitige Abschottung der IT-/OT-Umgebung sowie der S-MSR
- Fernzugriffsmöglichkeiten (z. B. über das Internet) müssen geschützt werden

Regelungen zu Zugang und Zugriff
- Physischer Zugang nur für Berechtigte, z. B. durch physische Barrieren (Zäune, Räume, Schränke etc.)
- Logischer Zugang nur nach Authentifizierung, z. B. Token / Dongle oder Passwörter

Härtung von Komponenten
- Hard- und Software auf die funktionalen Mindestanforderungen reduzieren (aber nicht weniger!)
- Unnötige Schnittstellen, Funktionen, Applikationen und Dienste deaktivieren oder entfernen

Unabhängigkeit von sicherheitsrelevanten MSR-Einrichtungen
- Keine unzulässige Beeinflussung durch die IT-/OT-Umgebung
- Möglichst Safetysyteme von betrieblichen Systemen trennen

Überwachung
- Protokollierung und Auswertung des Zustands der S-MSR und IT-/OT-Umgebung
- Schutz der Überwachungs- und Protokolldaten vor unberechtigter Änderung

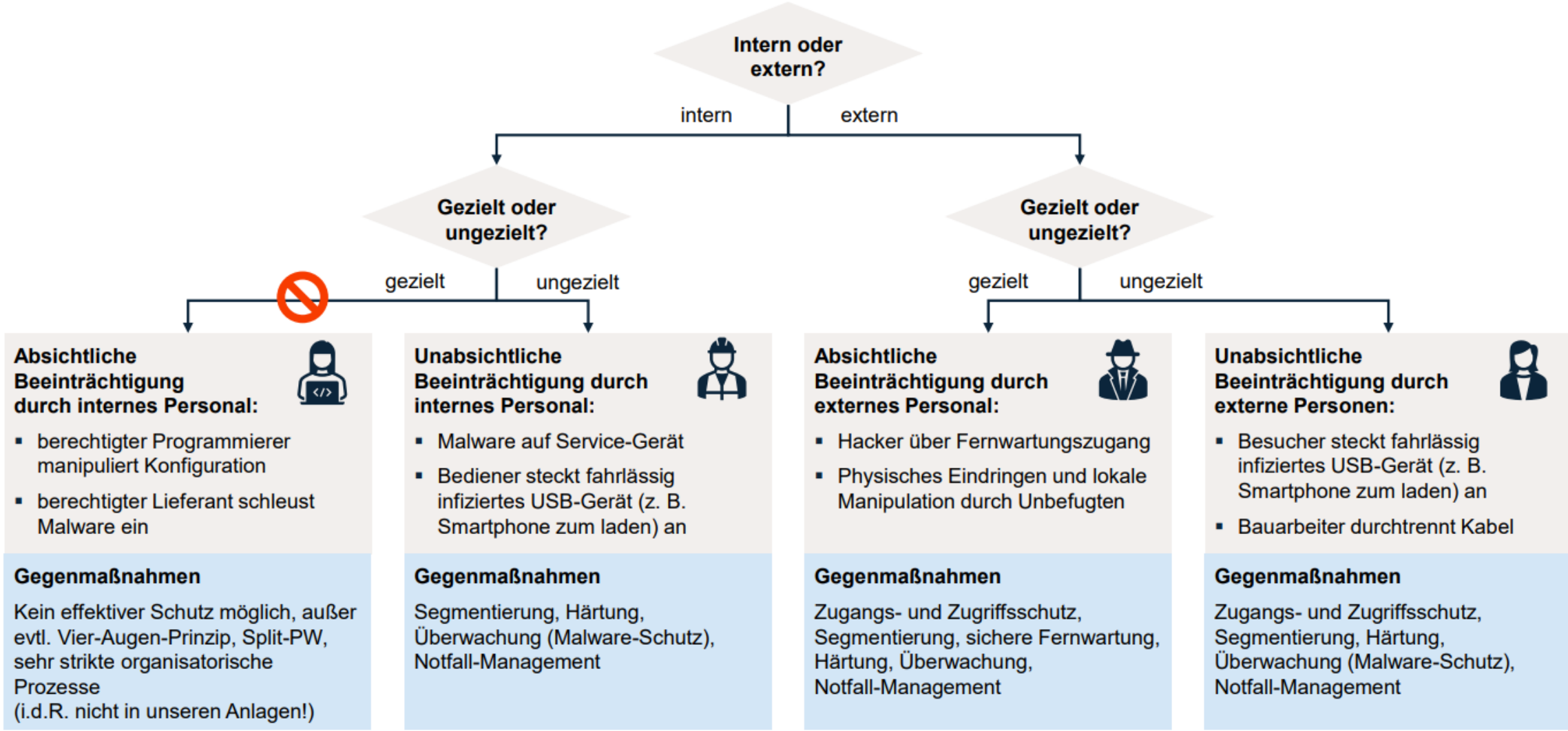
Notfallmanagement
- Festlegung von Maßnahmen zur Behandlung von Security-Vorfällen in S-MSR und IT-/OT-Umgebung
- Notfallplan unter Berücksichtigung nicht-digitaler Maßnahmen und Bereinigung vor der Wiederinbetriebnahme

Präventive Maßnahmen

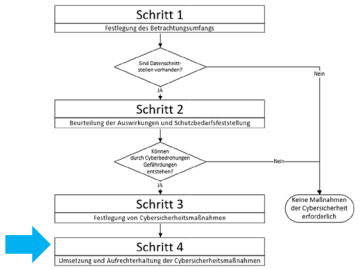
Detektive Maßnahmen

Reaktive Maßnahmen

Schritt 3:Cybersicherheitsmaßnahmen und Täter



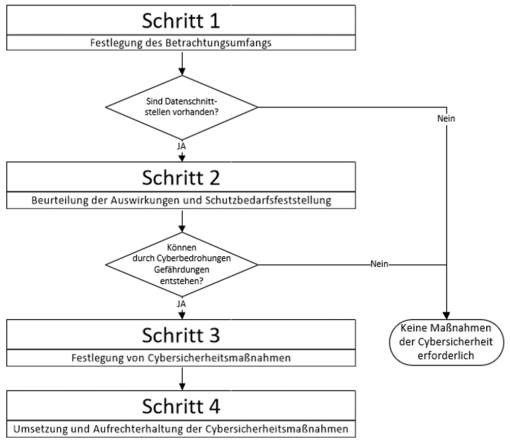
Schritt 4: Umsetzung und Aufrechterhaltung Cybersicherheitsmaßnahmen



- Technische Maßnahmen wie geplant implementieren
- Funktionsfähigkeit feststellen
- Unzulässige Rückwirkungen ausschließen
- Organisatorische Maßnahmen wie geplant implementieren
- Anweisungen in Kraft setzen
- Mitarbeiter unterweisen

Wirksamkeit feststellen

Kleiner Exkurs zur Wirksamkeit



Wirksam

Wenn der Weg passt, ist das Ergebnis gut. (TRBS 1115-1)

Unabhängiger Nachweis eines anforderungsgerechten Ergebnisses (Klassische Cybersecurity)

Schritt 4: Umsetzung und Aufrechterhaltung der Cybersicherheitsmaßnahmen

3 Anforderungen der Cybersicherheit an sicherheitsrelevante MSR-Einrichtungen

3.1 Allgemeines

(…)

(5) Zur Erfüllung der Vorgaben des § 3 Absatz 7 BetrSichV in Verbindung mit § 4 Absatz 6 BetrSichV sind Verfahren zu etablieren, um die Eignung und Funktionsfähigkeit der Cybersicherheitsmaßnahmen

1. regelmäßig in geeigneten Zeitabständen,
2. bei Änderungen am Arbeitsmittel (siehe hierzu Abschnitt 8.3),
3. bei neuen Erkenntnissen zu Cyberbedrohungen z. B. aus veröffentlichten oder firmeninternen Cybersicherheitsvorfällen und Schwachstellenmeldungen oder aus einschlägigen Veröffentlichungen,
4. bei Änderungen des Stands der Technik der Cybersicherheit

zu überprüfen.

Eine Regelmäßigkeit / Frequenz (z. B. einmal pro Jahr) sollte festgelegt sein

Anlassbezogen, z. B. nach Einbringung eines neuen Systems

Z. B. durch E-Mail-Abonnement der Herstellermeldungen (Siemens, ABB, Bosch, …)

Z. B. Systeme zur Angriffserkennung als neue Cybersicherheitsmaßnahme in KRITIS

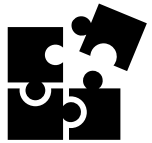
Unsere Agenda

Wichtige Begriffe und Grundlagen

Die TRBS 1115-1

Umsetzung der Cybersecurity

Prüfung durch die ZÜS



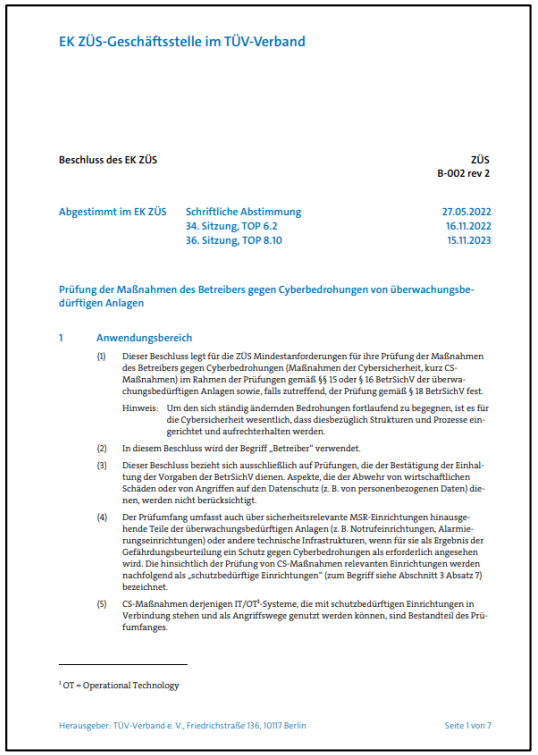
Prüfung der Maßnahmen der Cybersicherheit durch die ZÜS

Bisher war durch die ZÜS gemäß Beschluss des EK-ZÜS nur zu prüfen, ob im Rahmen der GBU durch den Betreiber eine dokumentierte Behandlung des Themas „Cybersecurity“ erfolgt ist.

Zukünftig wird zur Feststellung der Eignung von CS-Maßnahmen eine Plausibilitätsprüfung der Prozesse zu deren Planung und Realisierung durchgeführt. (Ordnungsprüfung)

Ergeben sich hierbei Defizite, wird ein geringfügiger Mangel ausgesprochen.

Verpflichtend für alle ZÜS-Prüforganisationen



EK ZÜS-Geschäftsstelle im TÜV-Verband

Beschluss des EK ZÜS — ZÜS B-002 rev 2

Abgestimmt im EK ZÜS	Schriftliche Abstimmung	27.05.2022
	34. Sitzung, TOP 6.2	16.11.2022
	36. Sitzung, TOP 8.10	15.11.2023

Prüfung der Maßnahmen des Betreibers gegen Cyberbedrohungen von überwachungsbedürftigen Anlagen

1 Anwendungsbereich

(1) Dieser Beschluss legt für die ZÜS Mindestanforderungen für ihre Prüfung der Maßnahmen des Betreibers gegen Cyberbedrohungen (Maßnahmen der Cybersicherheit, kurz CS-Maßnahmen) im Rahmen der Prüfungen gemäß §§ 15 oder § 16 BetrSichV der überwachungsbedürftigen Anlagen sowie, falls zutreffend, der Prüfung gemäß § 18 BetrSichV fest.

Hinweis: Um den sich ständig ändernden Bedrohungen fortlaufend zu begegnen, ist es für die Cybersicherheit wesentlich, dass diesbezüglich Strukturen und Prozesse eingerichtet und aufrechterhalten werden.

(2) In diesem Beschluss wird der Begriff „Betreiber“ verwendet.

(3) Dieser Beschluss bezieht sich ausschließlich auf Prüfungen, die der Bestätigung der Einhaltung der Vorgaben der BetrSichV dienen. Aspekte, die der Abwehr von wirtschaftlichen Schäden oder von Angriffen auf den Datenschutz (z. B. von personenbezogenen Daten) dienen, werden nicht berücksichtigt.

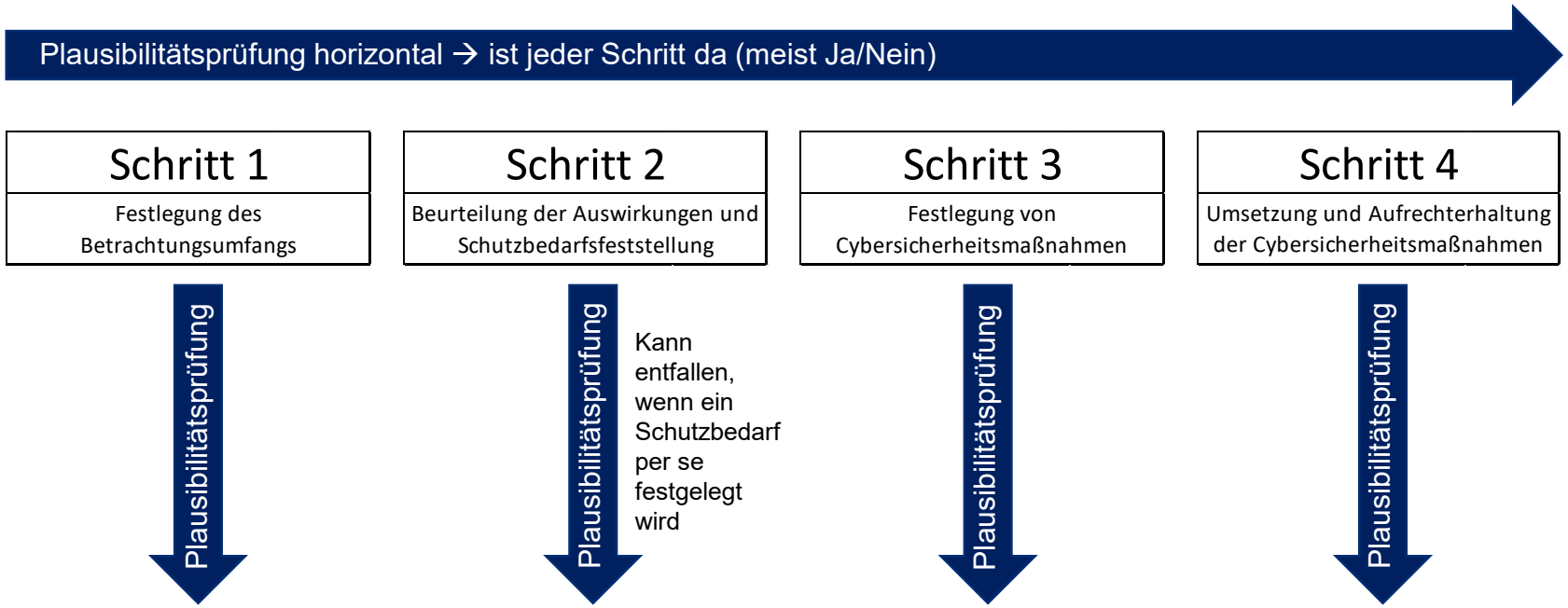
(4) Der Prüfumfang umfasst auch über sicherheitsrelevante MSR-Einrichtungen hinausgehende Teile der überwachungsbedürftigen Anlagen (z. B. Notrufeinrichtungen, Alarmierungseinrichtungen) oder andere technische Infrastrukturen, wenn für sie als Ergebnis der Gefährdungsbeurteilung ein Schutz gegen Cyberbedrohungen als erforderlich angesehen wird. Die hinsichtlich der Prüfung von CS-Maßnahmen relevanten Einrichtungen werden nachfolgend als „schutzbedürftige Einrichtungen“ (zum Begriff siehe Abschnitt 3 Absatz 7) bezeichnet.

(5) CS-Maßnahmen derjenigen IT/OT[1]-Systeme, die mit schutzbedürftigen Einrichtungen in Verbindung stehen und als Angriffswege genutzt werden können, sind Bestandteil des Prüfumfanges.

[1] OT = Operational Technology

Herausgeber: TÜV-Verband e. V., Friedrichstraße 136, 10117 Berlin — Seite 1 von 7

Prüfung der Maßnahmen der Cybersicherheit durch die ZÜS



Plausibilitätsprüfung vertikal → entsprechen die Ergebnisse des Schritts (Dokumentation) dem, was ich erwarte? (Stichprobe hinsichtlich Vollständigkeit und Richtigkeit)

Mögliche Fragen eines ZÜS-Prüfers

Schritt 1
Festlegung des Betrachtungsumfangs

- Sind alle S-MSR Einrichtungen, Anfangsteile mit Sicherheitsfunktion oder Anlagenteile, die bei Cyberbedrohungen Auswirkungen auf den sicheren Zustand der Anlage haben könnten, in ihrem Betrachtungsumfang?
- Gibt es eine Erfassung aller datentechnischen Schnittstellen?

Schritt 2
Beurteilung der Auswirkungen und Schutzbedarfsfeststellung

- Wurden mögliche Folgen einer Manipulation für die Systeme im Betrachtungsumfang ermittelt und festgestellt, ob Gefährdungen entstehen können?
- Wird der Schutzbedarf anhand des Ausmaßes möglicher Folgen abgestuft? Wenn ja, wie?
- Sind die schutzbedürftigen Systeme als solche festgeschrieben?

(Bei Bedarf Durchführung einer Stichprobe der zugehörigen Dokumentation auf Vollständigkeit und Richtigkeit)

Mögliche Fragen eines ZÜS-Prüfers

Schritt 3

Festlegung von Cybersicherheitsmaßnahmen

- Wurden die Standardmaßnahmen der TRBS 1115-1 Abschnitt 4.5.2 Absatz 2 im erforderlichen Umfang berücksichtigt?
- Wurden die erforderlichen CS-Maßnahmen festgeschrieben?
- Werden Herstellervorgaben (wenn vorhanden) berücksichtigt?
- Wird ein Verfahren zur Aufrechterhaltung des Cybersicherheitsniveaus etabliert?

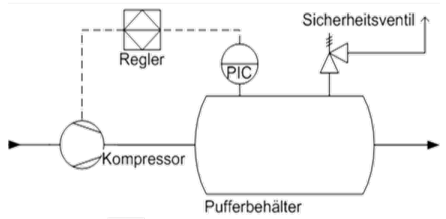
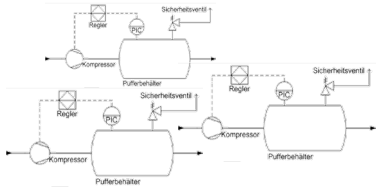
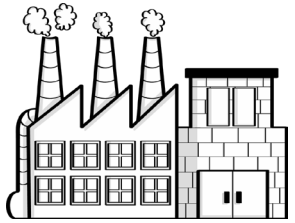
Schritt 4

Umsetzung und Aufrechterhaltung der Cybersicherheitsmaßnahmen

- Sind organisatorische Maßnahmen der Cybersicherheit in einer Betriebsanweisung festgeschrieben und ist das Personal unterwiesen?
- Wurde die Funktionsfähigkeit/Wirksamkeit der technischen Maßnahmen der Cybersicherheit überprüft?

(Bei Bedarf Durchführung einer Stichprobe der zugehörigen Dokumentation auf Vollständigkeit und Richtigkeit)

Ein Prozess, unterschiedliche Ausprägungen

Einzelne oder kleine Anlagen	Viele oder sehr große Anlagen	Unternehmen mit ISMS
		
Einzelbehand-lung des Systems	Regelbasierte Bearbeitung	Prozessbasierte Bearbeitung
z.B.: Einzeldoku-mentation	Dokumentationssystem mit Summenbildungen	Asset-Management
…	…	…

⇨ Die Prüfung orientiert sich an dem System des Betreibers, wichtig ist, dass ausreichende Informationen für eine Prüfung vorhanden sind.

Wie sieht es denn mit den Mängeln aus?

	zur Orientierung		Angemessene Reaktion des Betreibers	
Mängel in der Dokumentation oder in den Maßnahmen der Cybersicherheit (die nicht erheblich sind)	→	Geringfügiger Mangel	→	**Angemessen** und **sorgfältig** Nacharbeiten
Es gibt (vermutlich) ungeschützte Verbindungen von schutzbedürftigen Systemen in unzureichend geschützten Bereichen (in die Außenwelt)	→	Erheblicher Mangel	→	**Schnellstmöglich** beheben
Schutzbedürftige Systeme wurden bereits kompromittiert. Das Eintreten einer Gefährdung ist jederzeit möglich.	→	Gefährlicher Mangel	→	**Abschalten** und Problem beheben

Fragen, Diskussionen, weitere Beispiele

Kontakt

Jörg Becker
089 5791-1475
joerg.becker@tuvsud.com

Mehr Wert.
Mehr Vertrauen.