TRBS 1115-1

Cybersicherheit für sicherheits- relevante Mess-, Steuer- und Regeleinrichtungen

Ralf.Schmitt@de.tuv.com

TÜVRheinland®
Genau. Richtig.

Agenda

Kapitel	Thema	Dauer	Referent	Seite
1	Einführung			
2	Anwendungsbereich			
3	Begriffe			
4	Anforderungen allgemein			
5	Fachkunde			
6	Wann sind Cyberbedrohungen relevant ?			
7	Anforderungen Gefährdungsbeurteilung			
8	Planung und Realisierung			
9	Überprüfung und Prüfung			

Einführung

Einführung

Hello, this is the CL0P hacker group. As you may know, we recently carried out a hack, which was reported in the news on site [redacted].
We want to inform you that we have stolen important information from your GoAnywhere MFT resource and have attached a full list of files as evidence.
We deliberately did not disclose your organization and wanted to negotiate with you and your leadership first. If you ignore us, we will sell your information on the black market and publish it on our blog, which receives 30-50 thousand unique visitors per day. You can read about us on [redacted] by searching for CLOP hacker group.
You can contact us using the following contact information:
unlock@rsv-box[.]com
and
unlock@support-mult[.]com

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Framework für Angriffe auf ICS- und SCADA-Systeme (INCONTROLLER / PIPEDREAM)

CSW-Nr. 2022-215481-1032, Version 1.0, 14.04.2022

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:WHITE: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP" zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

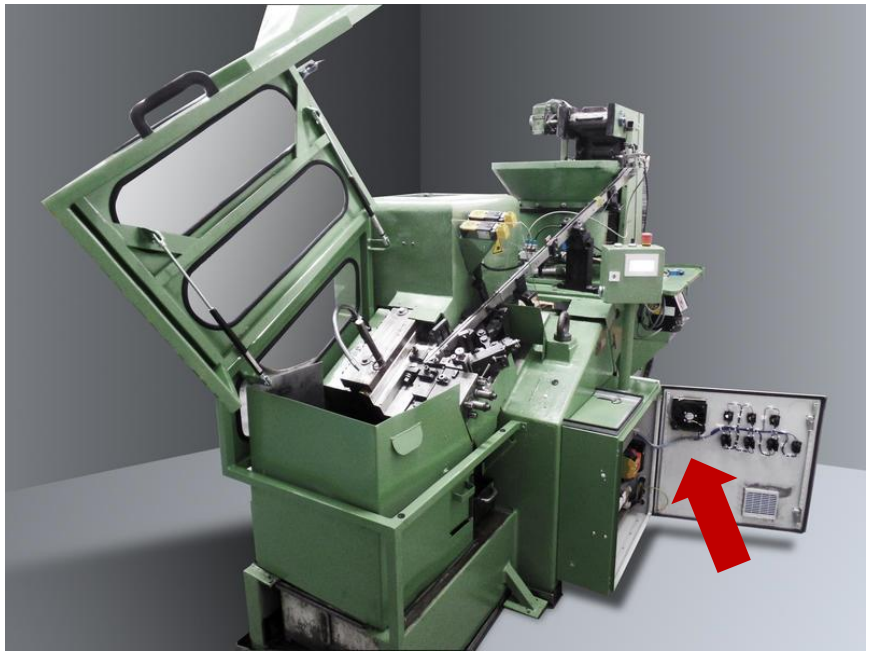
Sachverhalt

Am 13.4.2022 wurde durch die US-Behörden CISA, DOE, NSA und FBI ein gemeinsames Security Advisory veröffentlicht, welches verschiedene Tools beschreibt, die zum Einsatz gegen industrielle Steuerungs- und Automatisierungssysteme entwickelt wurden [CIS2022]. Die Firma Dragos verwendet den Namen "PIPEDREAM" [DRA2022]. Mandiant bezeichnet in seinem Bericht das Toolkit als "INCONTROLLER" [MAN2022].

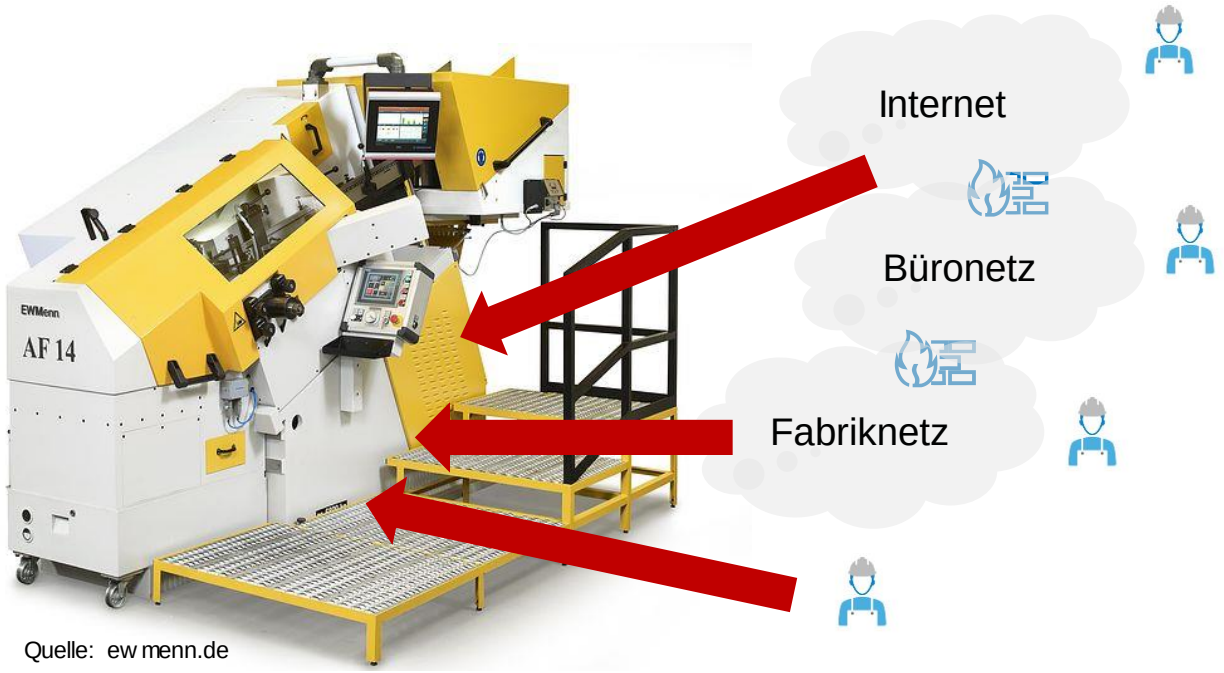
Das Framework besteht aus den folgenden Komponenten, die gemeinsam oder unabhängig voneinander eingesetzt werden können:

Einführung

Was hat sich verändert?



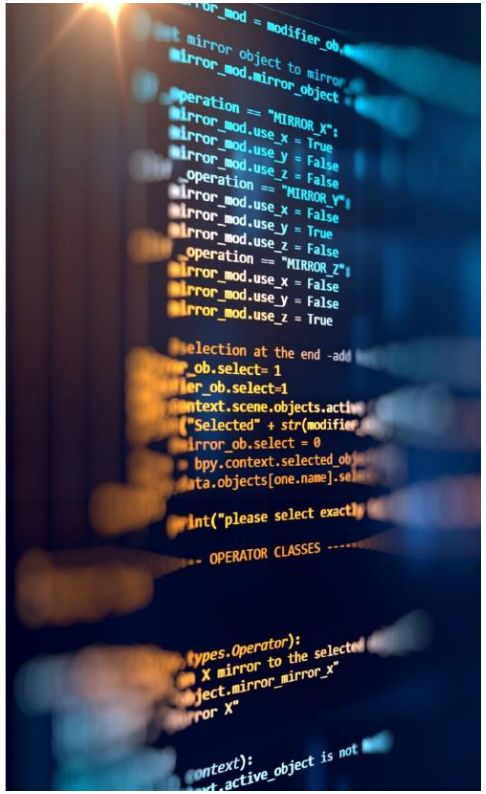
Quelle: cse-berlin.de



Quelle: ew menn.de

Einführung

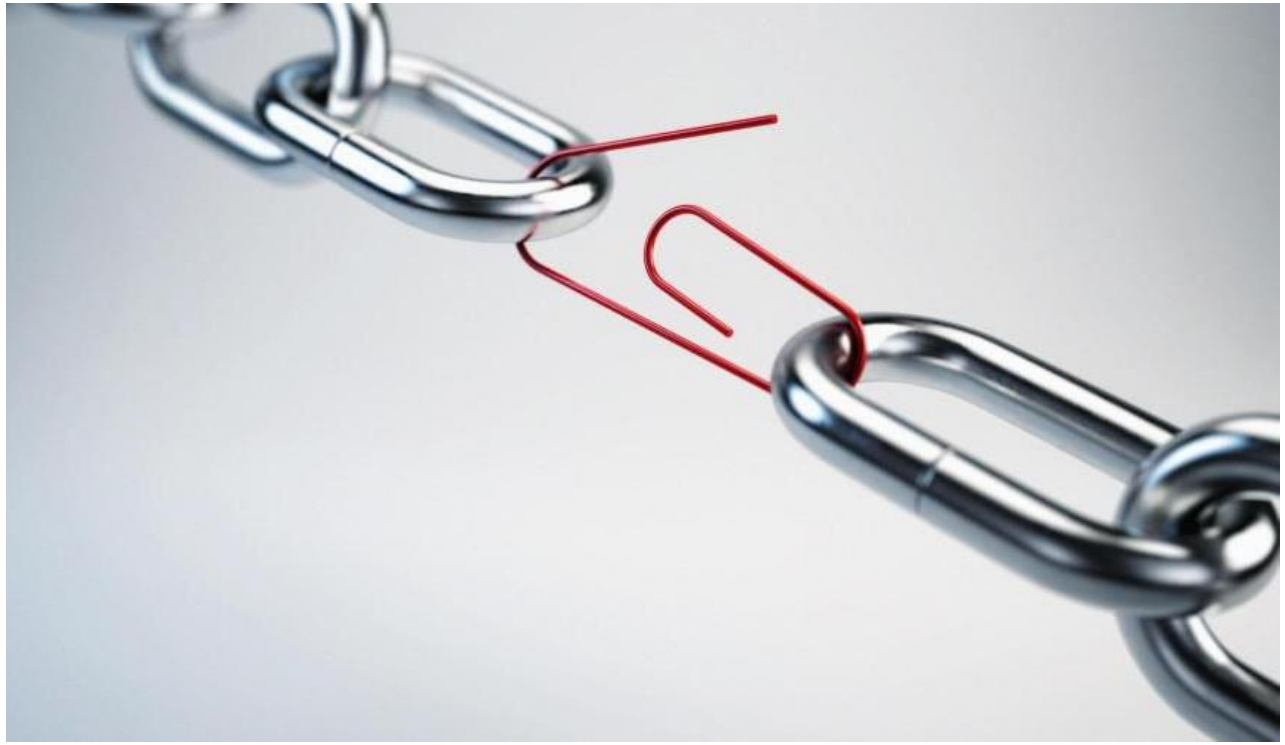
Wie viele Sprachen sehen Sie?



TÜVRheinland®
Genau. Richtig.

Einführung

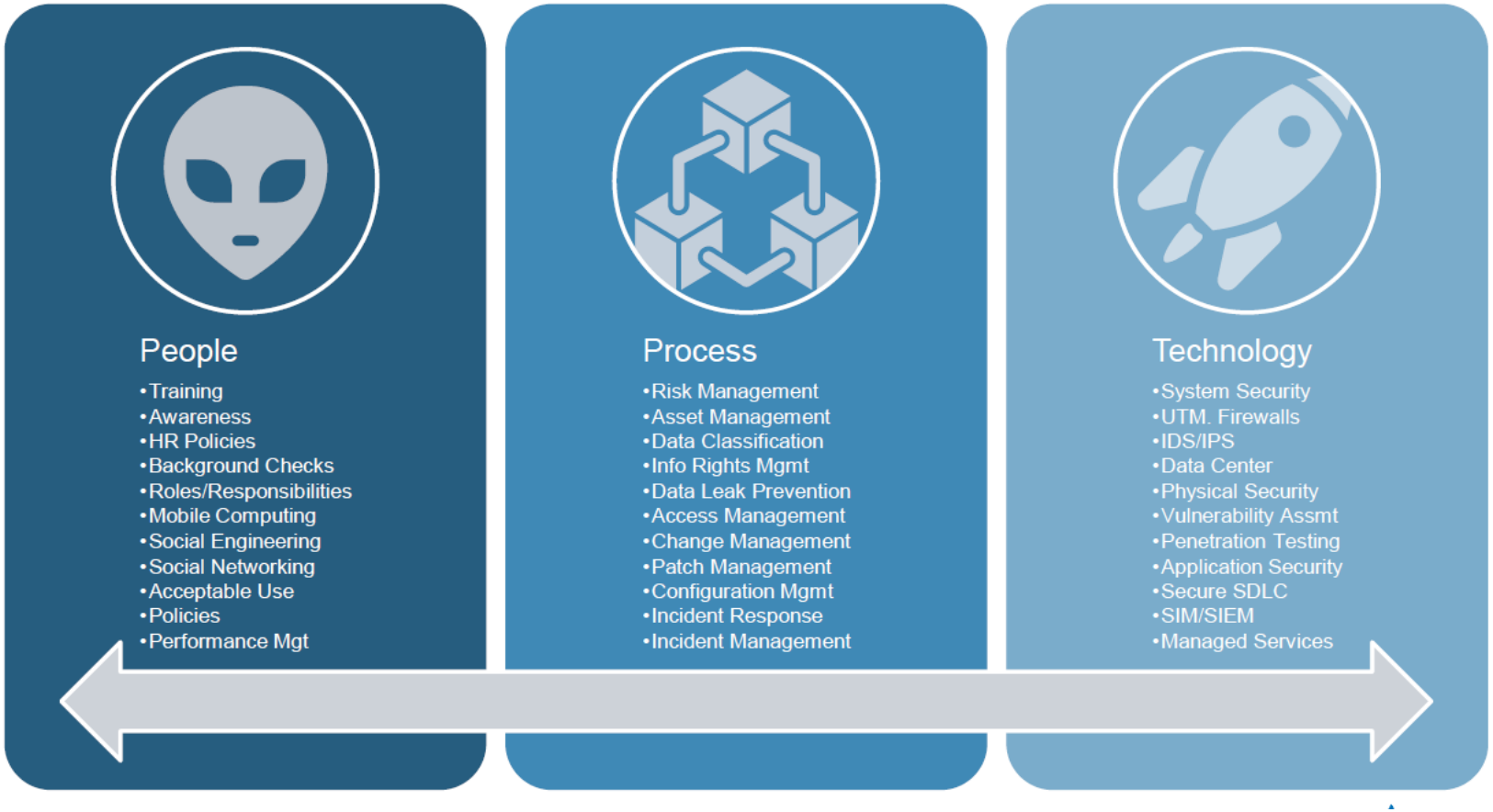
Was hat Einfluss auf die Cybersicherheit?



- Der Mensch
- Das Team
- Das Ziel
- Das Bugdet
- Die Vorgaben

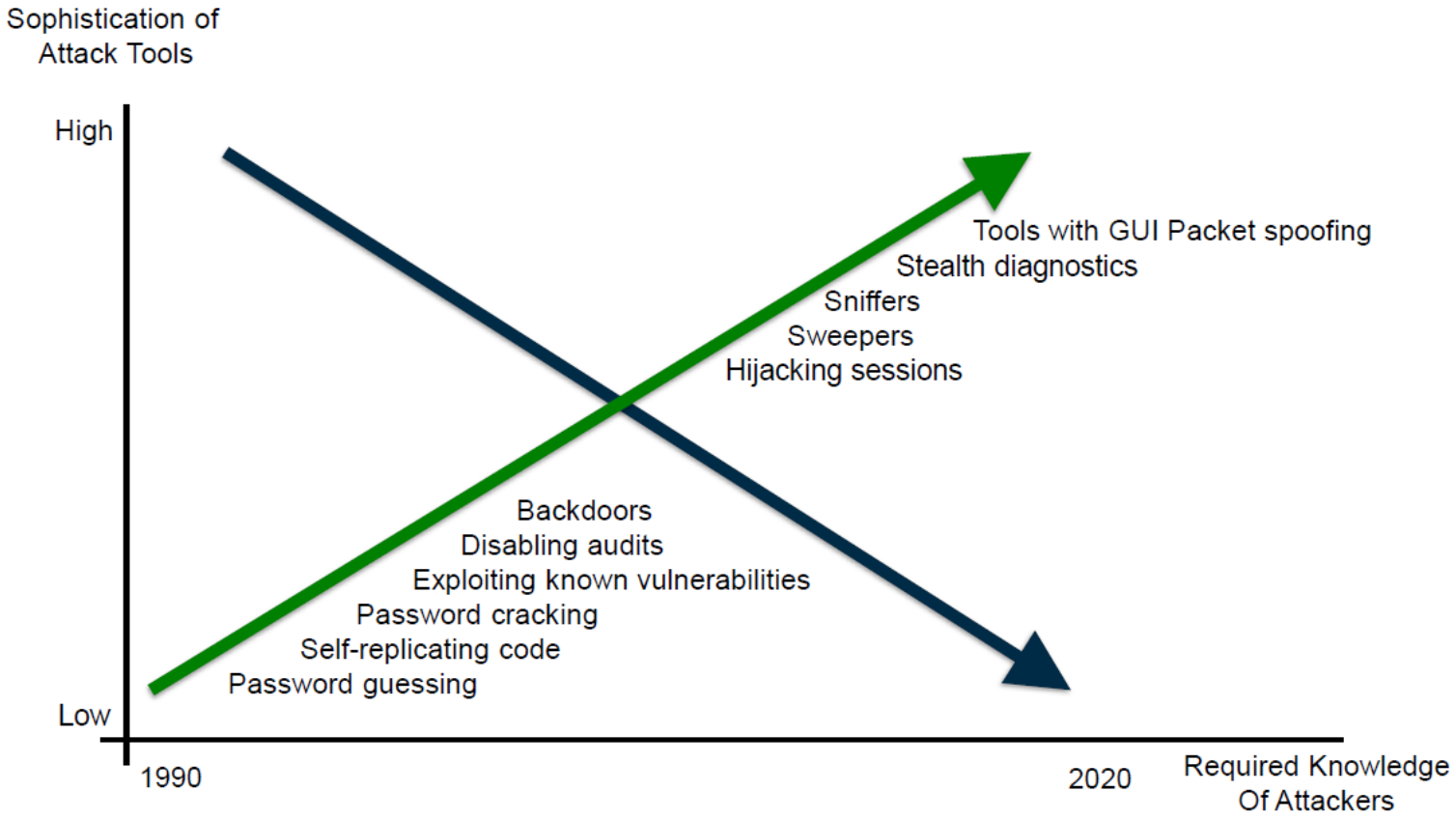
Einführung

Der Dreiklang der Cybersicherheit



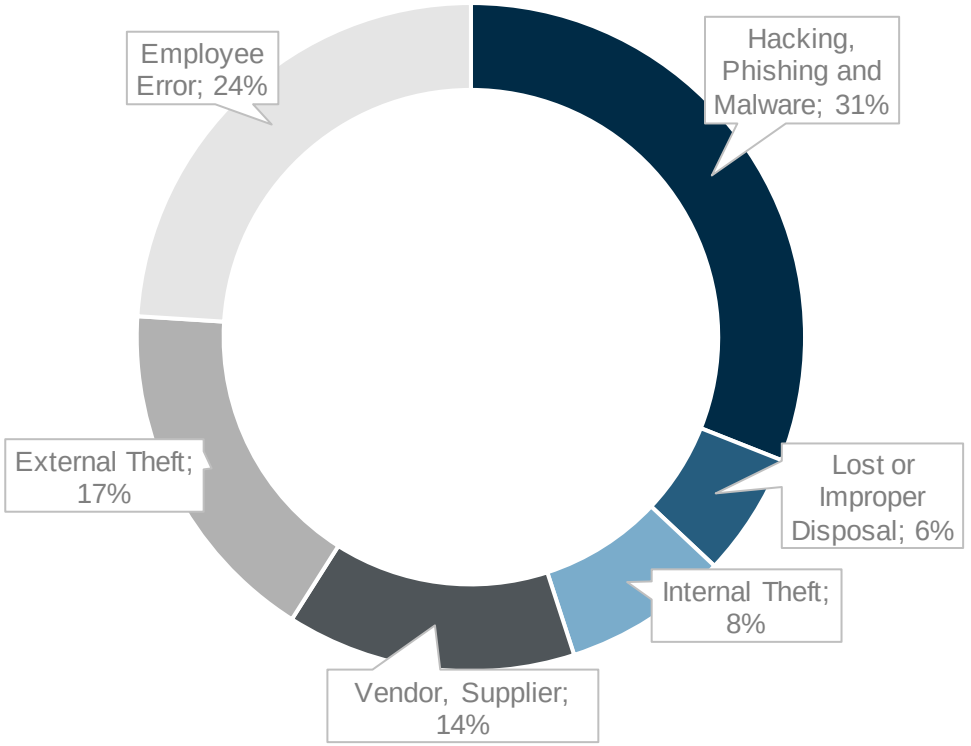
Einführung

Wie habe sich die Bedrohungen entwickelt?



Einführung

Wie habe sich die Bedrohungen entwickelt?



Source: 2016 Data Security Incident Response Report

Einführung

Helfer der Hacker

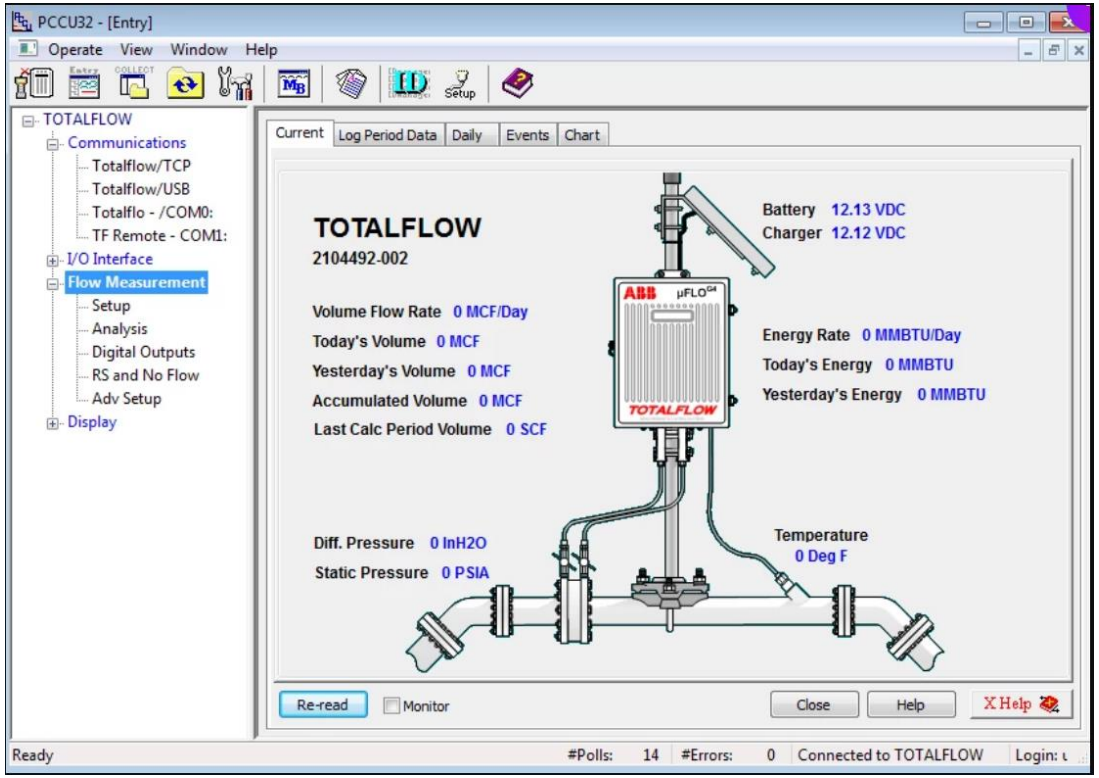
ALIExpress.com

Amazon.de

TÜVRheinland®
Genau. Richtig.

Einführung

Reale Gefährdung



November 10, 2022 By Pierluigi Paganini Posted In Breaking News Security

Forscher des Industrie-Sicherheitsunternehmens Claroty haben Einzelheiten über eine Schwachstelle bekannt gegeben, die ABB Totalflow-Durchflussrechner und Fernsteuerungen betrifft. Durchflussrechner werden zur Berechnung von Volumen und Durchflussraten für Öl und Gas verwendet, die für die Stromerzeugung und -verteilung von entscheidender Bedeutung sind.

Die kritischen Systeme werden von Öl- und Gasunternehmen auf der ganzen Welt eingesetzt. Bei der Sicherheitslücke handelt es sich um ein Pfadumgehungsproblem, das von einem Angreifer ausgenutzt werden kann, um beliebigen Code einzuschleusen und auszuführen.

Angreifer können diese Schwachstelle ausnutzen, um Root-Zugriff auf einen ABB-Flow-Computer zu erhalten, Dateien zu lesen und zu schreiben und Code aus der Ferne auszuführen.

Agenda

Kapitel	Thema	Dauer	Referent	Seite
1	Einführung			
2	Anwendungsbereich			
3	Begriffe			
4	Anforderungen allgemein			
5	Fachkunde			
6	Wann sind Cyberbedrohungen relevant ?			
7	Anforderungen Gefährdungsbeurteilung			
8	Planung und Realisierung			
9	Überprüfung und Prüfung			

TRBS 1115 Teil 1

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

Technische Regel für Betriebssicherheit	**Cybersicherheit für sicherheits-relevante 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.

TRBS 1115 Teil 1

1. Anwendungsbereich

Die TRBS

1. konkretisiert die 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.
2. beschreibt die Durchführung von Prüfungen zur Cybersicherheit sowie das Vorgehen bei Änderungen von Arbeitsmitteln im Zusammenhang mit der Cybersicherheit von sicherheitsrelevanten MSR-Einrichtungen.
3. behandelt keine Arbeitsmittel oder sicherheitsrelevanten MSR-Einrichtungen, die aufgrund nicht vorhandener Schnittstellen (sowohl kabelgebunden als auch kabellos) nicht kompromittiert werden können.

   Als auch die Abwehr von wirtschaftlichen Schäden oder von Angriffen auf den Datenschutz (z. B. von personenbezogenen Daten).

TRBS 1115 Teil 1

1. Anwendungsbereich

Grundsätzlich geht die Betrachtung der Cybersicherheit über die sicherheitsrelevanten MSR-Einrichtungen hinaus

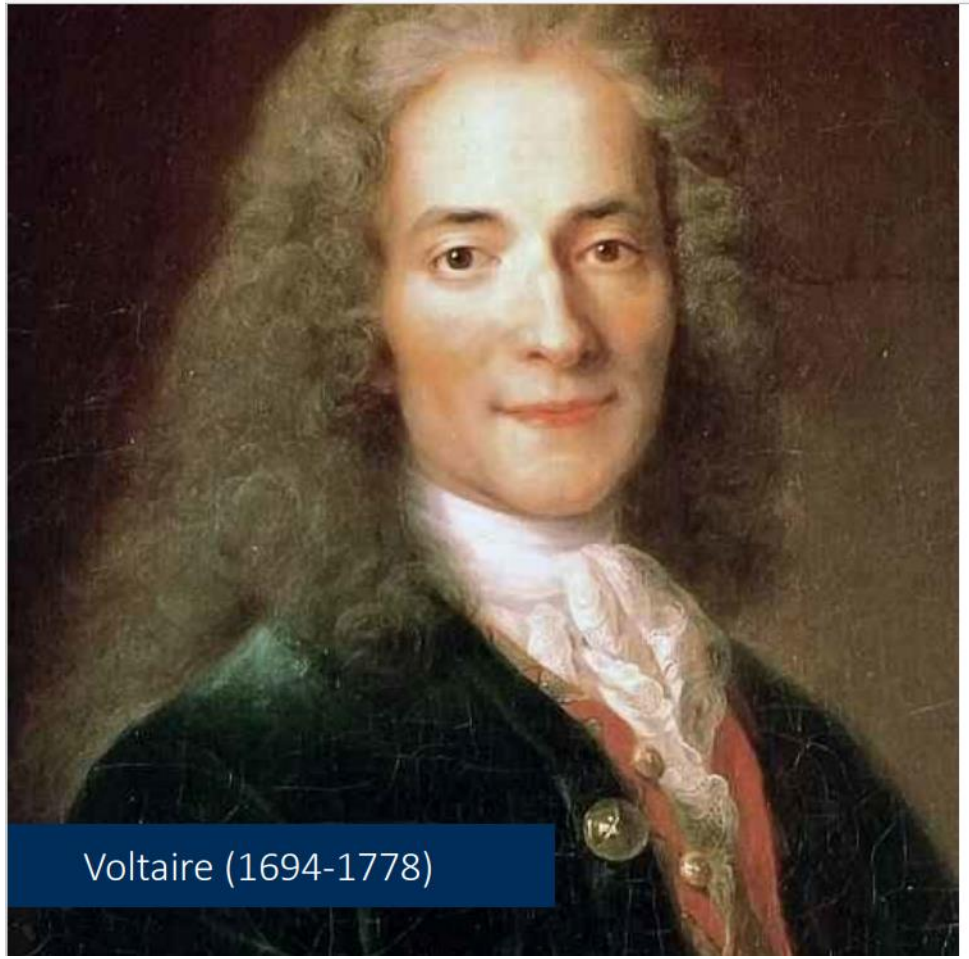
…

wenn im Ergebnis der Gefährdungsbeurteilung es als erforderlich angesehen wird, dass über sicherheitsrelevante MSR-Einrichtungen hinausgehende Teile des Arbeitsmittels (z. B. notwendige Kommunikationsmittel) oder andere technische Infrastrukturen gegen Cyberbedrohungen zu schützen sind, können die dargestellten Vorgehensweisen zur Festlegung, Umsetzung und Prüfung von Cybersicherheitsmaßnahmen angewendet werden.

Agenda

Kapitel	Thema	Dauer	Referent	Seite
1	Einführung			
2	Anwendungsbereich			
3	Begriffe			
4	Anforderungen allgemein			
5	Fachkunde			
6	Wann sind Cyberbedrohungen relevant ?			
7	Anforderungen Gefährdungsbeurteilung			
8	Planung und Realisierung			
9	Überprüfung und Prüfung			

Begriffe



Si vous voulez discuter avec moi, définissez vos termes.

Wenn Sie mit mir diskutieren wollen, definieren Sie Ihre Begriffe!

Begriffe

Cybersicherheit

Der Begriff „Cybersicherheit“ im Sinne dieser TRBS beschränkt sich auf den Schutz sicherheitsrelevanter MSR-Einrichtungen, die als technische Schutzmaßnahme für die sichere Verwendung eines Arbeitsmittels inklusive einer überwachungsbedürftigen Anlage eingesetzt werden.

Cyberbedrohung

bezeichnet gem. Verordnung (EU) 2019/881 einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte.

IT-Systeme

sind die Hard- und Softwarekomponenten zur elektronischen Datenverarbeitung (IT - Information Technology).

OT-Systeme

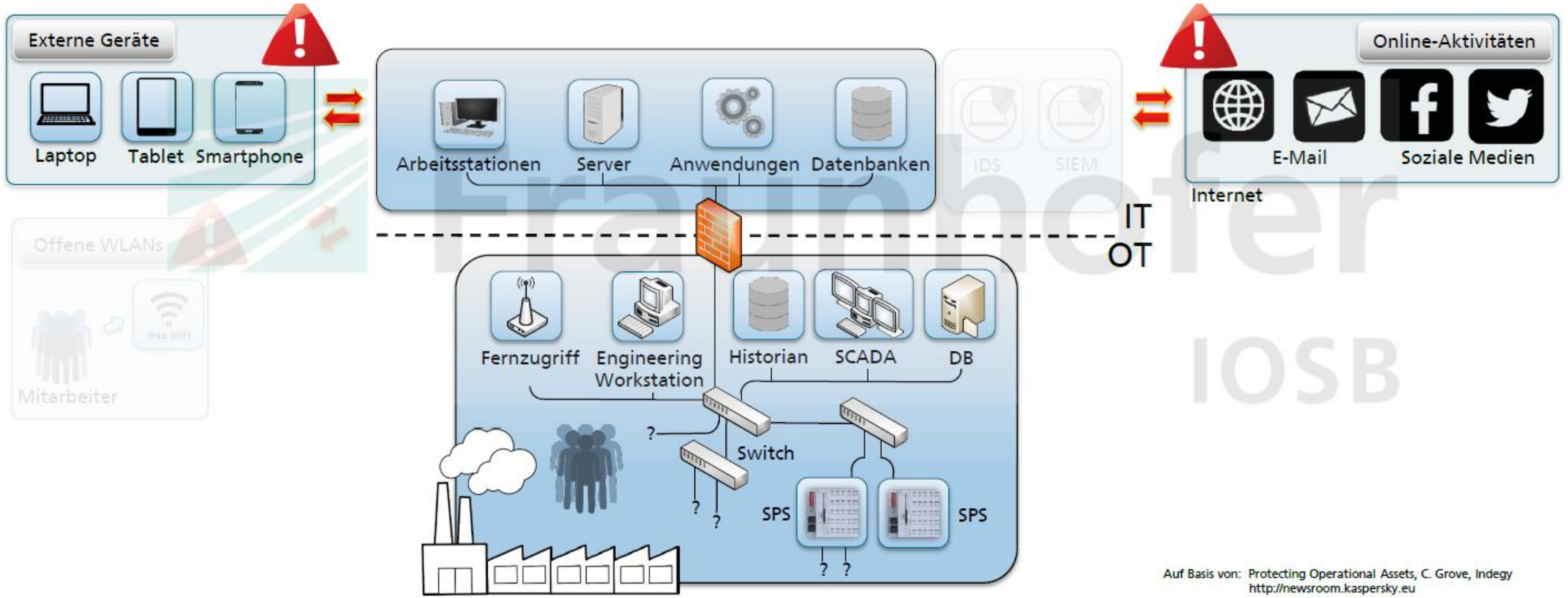
sind die Hard- und Softwarekomponenten zur Steuerung, Regelung, Überwachung und Kontrolle von Maschinen, Anlagen und Prozessen (OT - Operational Technology).

IT/OT-Umgebung

Die IT/OT-Umgebung bezeichnet die IT/OT-Systeme (Netz- und Informationssysteme im Sinne der Verordnung (EU) 2019/881), die temporär oder dauerhaft einen Informationsaustausch mit sicherheitsrelevanten MSR-Einrichtungen haben.

Begriffe

Wo fängt die IT an und wo die OT?



Quelle: Fraunhofer Institut

Funktionale Sicherheit in der Prozessindustrie

Begriffe

Hacker (Computersicherheit) – Wikipedia

Hacker

Hacker aus dem Bereich der Computersicherheit beschäftigen sich mit Sicherheitsmechanismen und deren Schwachstellen. Während der Begriff beinhaltet diejenigen, die Sicherheitslücken suchen, um sie aufzuzeigen als auch die, die die unerlaubt in fremde Systeme eindringen.

Staatlich unterstütze Hacker

Hacker die im Auftrag einer Regierung agieren, die hierfür speziell ausgebildet wurden und denen besonders komplexe Werkzeuge zur Verfügung stehen.

Scriptkiddies

Personen mit Grundwissen, die Versuchen mit einfachen Tools in Systeme einzudringen.

Begriffe

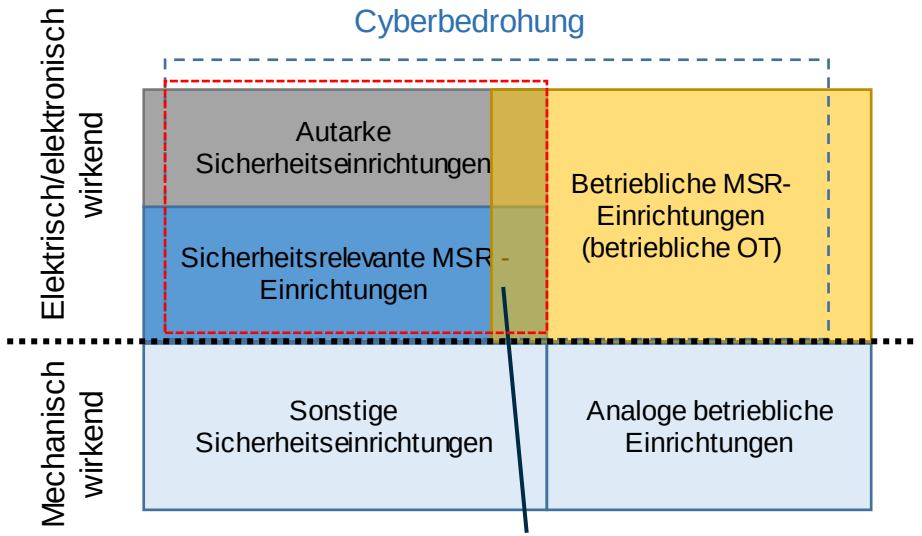
Ransomware

Es handelt sich um bösartige Software (Malware), die bei einem Cyberangriff verwendet wird, um die Daten des Opfers zu verschlüsseln.

Der Schlüssel ist nur dem Angreifer bekannt.

Begriffe

Assets



Schutzbedürftige -Einrichtungen
Betriebliche OT, die Rückwirkungen auf sicherheitsrelevante MSR- oder autarke Sicherheitseinrichtung haben kann.

Agenda

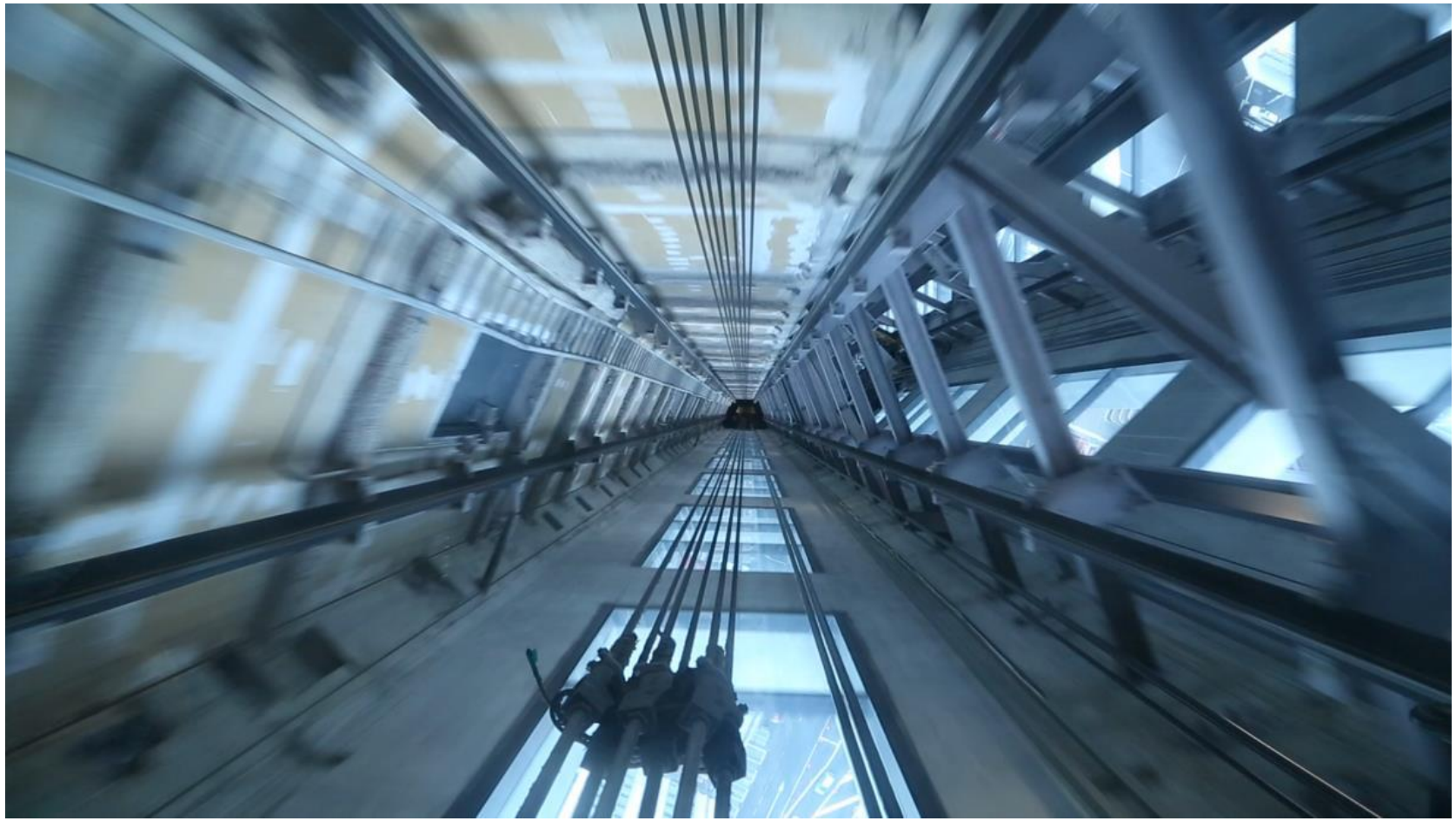
Kapitel	Thema	Dauer	Referent	Seite
1	Einführung			
2	Anwendungsbereich			
3	Begriffe			
4	Anforderungen allgemein			
5	Fachkunde			
6	Wann sind Cyberbedrohungen relevant ?			
7	Anforderungen Gefährdungsbeurteilung			
8	Planung und Realisierung			
9	Überprüfung und Prüfung			

Anforderungen allgemein

- Der Arbeitgeber hat nach § 3 BetrSichV die auftretenden Gefährdungen zu beurteilen und daraus notwendige Maßnahmen für das sichere Verwenden von Arbeitsmitteln abzuleiten.
- Im Rahmen der GBU und bei der Auswahl und Implementierung der sMSR-Einrichtungen sind auch Cyberbedrohungen zu berücksichtigen.
- SMSR-Einrichtungen, ihre Integration in das Arbeitsmittel und ihre Anwendung müssen nach dem Stand der Technik vor Cyberbedrohungen derart geschützt sein, dass Gefährdungen für Beschäftigte und bei überwachungsbedürftigen Anlagen auch andere Personen in deren Gefahrenbereich vermieden werden.

Anforderungen allgemein

Aufzugsanlagen



Anforderungen allgemein

Druckanlagen / Prozessanlagen

Anforderungen allgemein

Ex-Anlagen

Anforderungen allgemein

Tanklager

Anforderungen allgemein

Arbeitsmittel

Anforderungen allgemein

Technische Gebäudeausrüstung

Auch die technische Gebäudeausrüstung wie z.B.

- Lüftungsanlagen
- Brandmeldeanlagen

können relevant sein.

Anforderungen allgemein

Auswirkungen

Mögliche Auswirkungen von Cyberbedrohungen können sein

a. Beeinflussung der Verfügbarkeit
   z. B. Deaktivieren oder Blockieren der Funktion von sicherheitsrelevanten MSR-Einrichtungen,
   Eingriff in die Steuerung,
   Unterdrückung von Alarmierungen,

b. Verletzung der Integrität
   z. B. unberechtigte Änderung von

   Daten,
   Messwerte,
   Betriebsparameter,

c. Verletzung der Vertraulichkeit
   z. B. Abfluss von Daten einschließlich Passwörter und Signaturen

Anforderungen allgemein

Verfahren

Es sind Verfahren zu etablieren, um die Eignung und Funktionsfähigkeit der Cybersicherheitsmaßnahmen zu überprüfen bei:

- regelmäßig in geeigneten Zeitabständen,
- bei Änderungen am Arbeitsmittel,
- bei neuen Erkenntnissen zu Cyberbedrohungen z. B. aus veröffentlichten oder firmeninternen Cybersicherheitsvorfällen und Schwachstellenmeldungen oder aus einschlägigen Veröffentlichungen und
- bei Änderungen des Stands der Technik der Cybersicherheit

Anforderungen allgemein

Sicherheitslebenszyklus

Betroffen sind folgende Elemente:

- Hardware,
- Software,
- Daten/Informationen,
- Schnittstellen
- Prozesse,
- Richtlinien,
- Organisationen sowie
- Personen,
- IT/OT-Umgebung.

sowie die mit ihrer Verwendung verbundenen

Die Cybersicherheit muss während des gesamten Sicherheitslebenszyklus der sicherheitsrelevanten MSR-Einrichtung gewährleistet sein.

Agenda

Kapitel	Thema	Dauer	Referent	Seite
1	Einführung			
2	Anwendungsbereich			
3	Begriffe			
4	Anforderungen allgemein			
5	Fachkunde			
6	Wann sind Cyberbedrohungen relevant ?			
7	Anforderungen Gefährdungsbeurteilung			
8	Planung und Realisierung			
9	Überprüfung und Prüfung			

Fachkunde

Es ist erforderlich, Zugriffsrechte, Fachkunde (Qualifikation), Tätigkeiten, Verantwortlichkeiten, Zuständigkeiten und Aufgaben derjenigen Personen eindeutig festzulegen, die

- für den Auswahl-, Beschaffungs- und Integrationsprozess verantwortlich sind oder
- im Betrieb Umgang mit einer sicherheitsrelevanten MSR-Einrichtung und der IT/OT-Umgebung haben können (in der Regel auch die Verwender eines Arbeitsmittels).

Fachkunde

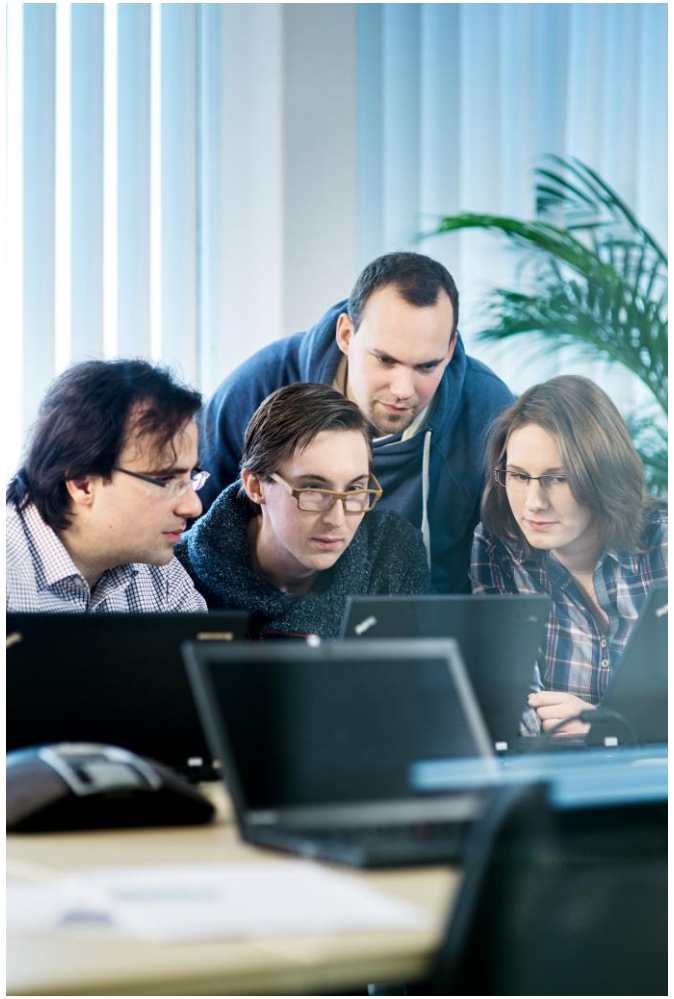
Welche Kenntnisse sind erforderlich?

Folgende Kenntnisse sind grundsätzlich erforderlich:

- gesetzlicher Anforderungen und Vorschriften sowie Normen zur Cybersicherheit
- im Bereich Cybersicherheit sowie Branchenkenntnisse
- über das jeweilige Unternehmen (z.B. Umgang mit Updates, Protokollierung, Überwachung)
- Managements der Cybersicherheit des Betriebs und die verwendeten Technologien notwendig. Dies sind unter anderem Prozesse zum Umgang mit Updates, Protokollierung, Überwachung.
- Maßnahmen zum Schutz vor Cyberbedrohungen

Fachkunde

Welche Kenntnisse sind erforderlich?



Falls der Arbeitgeber für eine sicherheitsrelevante MSR-Einrichtung eigenständig Cybersicherheitsmaßnahmen ermittelt und umsetzt, sind zusätzlich folgende Kenntnisse erforderlich:

- Informationssicherheitsmanagement,
- Vorgehensweisen zur Ermittlung von relevanten Cybergefährdungen auf Basis der Cyberbedrohungen und Schwachstellen,
- Vorgehensweisen zur systemspezifischen Auswahl von geeigneten Cybersicherheitsmaßnahmen, z. B.

  a. Hardwarearchitektur und Segmentierung
  b. Zugangs- und Zugriffskontrolle,
  c. sichere Installation und Änderung von Cybersicherheitsmaßnahmen,
  d. Funktionsreduktion und Härtung,
  e. Überwachung von Hardware, Software und ihrer Kommunikation,
  f. Notfallmanagement (z. B. response and recover, Disaster Recovery).

Agenda

Kapitel	Thema	Dauer	Referent	Seite
1	Einführung			
2	Anwendungsbereich			
3	Begriffe			
4	Anforderungen allgemein			
5	Fachkunde			
6	Wann sind Cyberbedrohungen relevant ?			
7	Anforderungen Gefährdungsbeurteilung			
8	Planung und Realisierung			
9	Überprüfung und Prüfung			

Wann sind Cyberbedrohungen relevant ?

1. Bei technischen Schutzmaßnahmen und ihre Folgefunktionen, sofern diese ausgerüstet bzw. ausgestaltet sind, mit:

   I. elektronischer Steuereinheit, sofern über diese sicherheitsrelevante MSR-Einrichtungen realisiert sind oder über diesen Einfluss auf Sicherheit der Anlage genommen werden kann
   II. Netzwerkanbindungen (kabelgebunden oder nicht kabelgebunden) oder
   III. zugänglichen Wartungs- oder Konfigurierschnittstellen (wie z. B. USB- Schnittstelle, Funkempfänger)

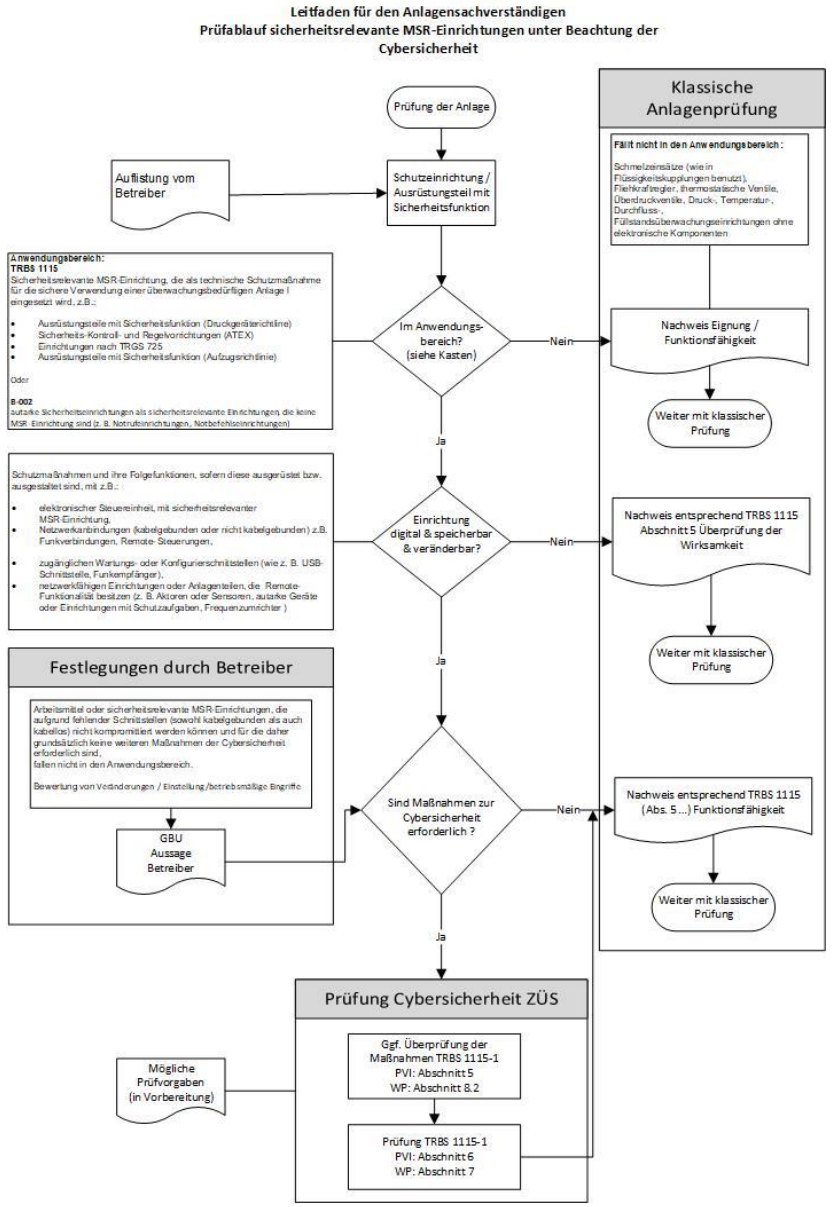
2. Bei netzwerkfähigen Einrichtungen oder Anlagenteilen sofern diese eine Remote-Funktionalität besitzen (z. B. MSR- Einrichtungen wie Aktoren oder Sensoren, autarke Geräte oder Einrichtungen mit Schutzaufgaben, haben, u. a. Frequenzumformer geregelte Antriebe)

3. Wenn Verbindungen mit öffentlichen Netzzugängen, wie Funkverbindungen, Benachrichtigung, Remote-Steuerungen, realisiert werden können.

Grundsätzlich sind keine weiteren Maßnahmen der Cybersicherheit erforderlich, wenn aufgrund fehlender Schnittstellen (sowohl kabelgebunden als auch kabellos) Arbeitsmittel und sicherheitsrelevante MSR-Einrichtungen nicht kompromittiert werden können.

Wann sind Cyberbedrohungen relevant ?

Ablaufbaum



Wann sind Cyberbedrohungen relevant ?

Beispiel 1

Befinden wir uns im Anwendungsbereich?

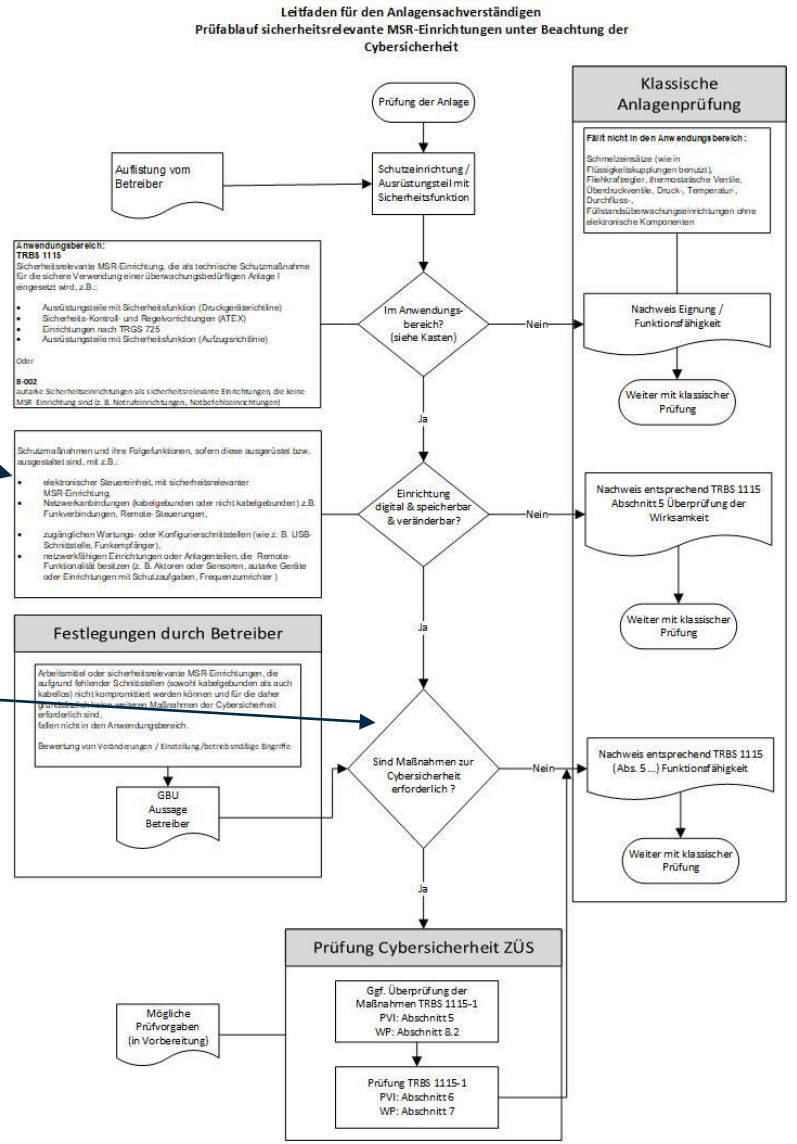
➔ Ja, sicherheitsrelevante MSR-Einrichtung vorhanden.

Sind die Einrichtungen digital & speicherbar & veränderbar?

➔ Ja, elektr. Steuereinheit mit sicherheitsrelevanter MSR-Einrichtung, Netzwerkanbindungen (nicht kabelgebunden), zugängliche Wartungs- oder Konfigurationsschnittstellen. Der Servicetechniker vor Ort zeigte mir anhand seiner App auf dem Handy, wie er die komplette Anlage abschalten kann. Hat er auch dann demonstriert ☺. Die Druckschalter an den Verdichtern sind analog und müsste man vor Ort aber ändern. Aber er kann komplett auf die Steuerung der Anlage vom Handy drauf zugreifen. War bei …. Natürlich alles mit Passwörtern geschützt.

Sind Maßnahmen zur Cybersicherheit erforderlich?

➔ Ja, Überprüfung der Passwortsicherheit, Zugangsdaten, etc.



TÜVRheinland®
Genau. Richtig.

Wann sind Cyberbedrohungen relevant ?

Beispiel 2

Befinden wir uns im Anwendungsbereich?

➔ JA, sicherheitsrelevante MSR-Einrichtung, Ausrüstungsteile mit Sicherheitsfunktion (Wasserstandsbegrenzer, Druckbegrenzer, Temperaturbegrenzer).

Sind die Einrichtungen digital & speicherbar & veränderbar?

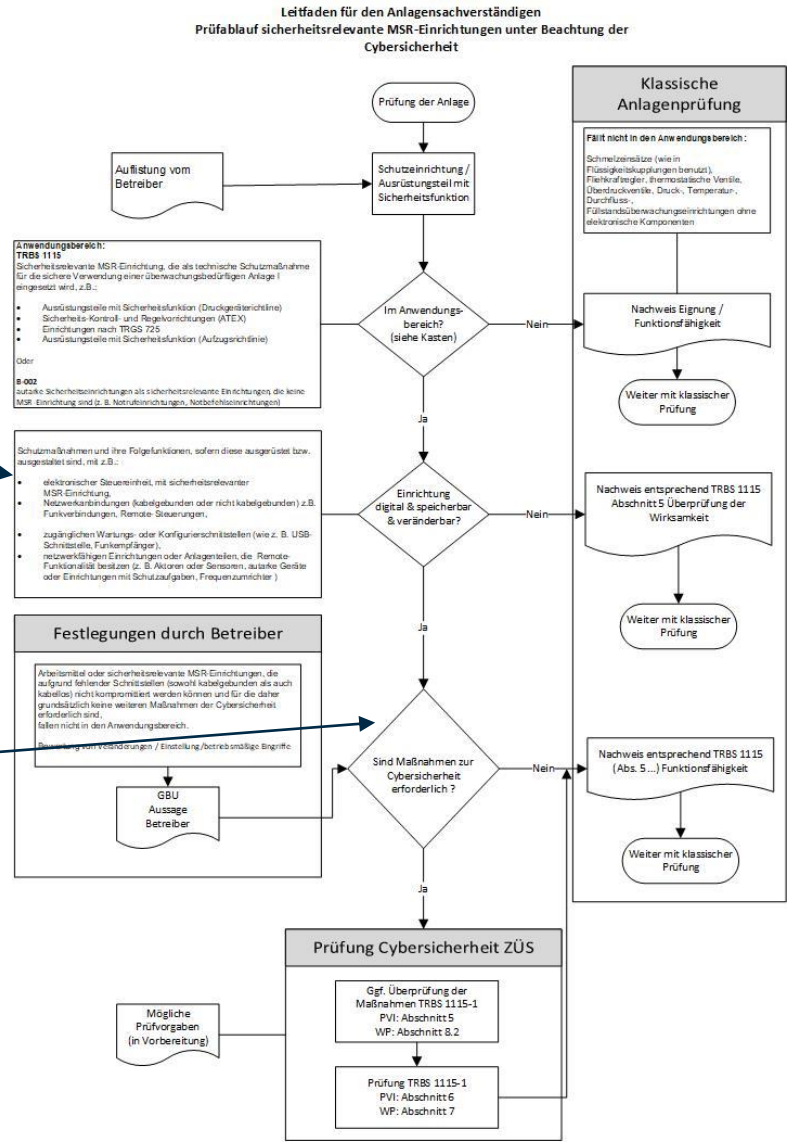
➔ Zum Teil ja (Druckbegrenzer, Temperaturbegrenzer). Netzwerkanbindung vorhanden (nicht kabelgebunden), Wartungsschnittstellen/Konfigurationsschnittstellen. Der Servicetechniker erklärte mir, dass er von der Ferne aus über eine Schnittstelle in ein Wartungssystem sich einwählen kann. Dort könnte er Werte und das System überprüfen. Grenzwerte verändern erfolgt laut seiner Aussage aber nur vor Ort. Der Mitarbeiter vom Krankenhaus hat „nur“ Zugriff auf das Anwenderprogramm (läuft über das Krankenhausnetzwerk). Hier können keine Werte verstellt werden.

➔ Bei einem der Elektrodampferzeuger war ein Druckschalter von Danfoss verbaut (siehe Bild unten). Fällt somit raus und geht in das Feld *Nachweis entsprechend TRBS 1115 Abschnitt 5 Überprüfung der Wirksamkeit -> Weiter mit klassischer Prüfung*

Sind Maßnahmen zur Cybersicherheit erforderlich?

➔ Fällt mir in diesem Fall schwer zu beurteilen. Eine Schnittstelle ist zwar vorhanden und Grenzwertgeber und Temperaturbegrenzer sind digital & speicherbar, aber da der Servicetechniker mir versicherte, dass nur vor Ort die Grenzwerte geändert werden können, tendiere ich eher zu Nein. Es gibt zwar eine Schnittstelle in das System. Allerdings unter der Voraussetzung, dass jemand vor Ort über das Bedienfeld den Zugang frei gibt. Des Weiteren müsste sich jemand in das Wartungssystem von MMM noch einwählen.

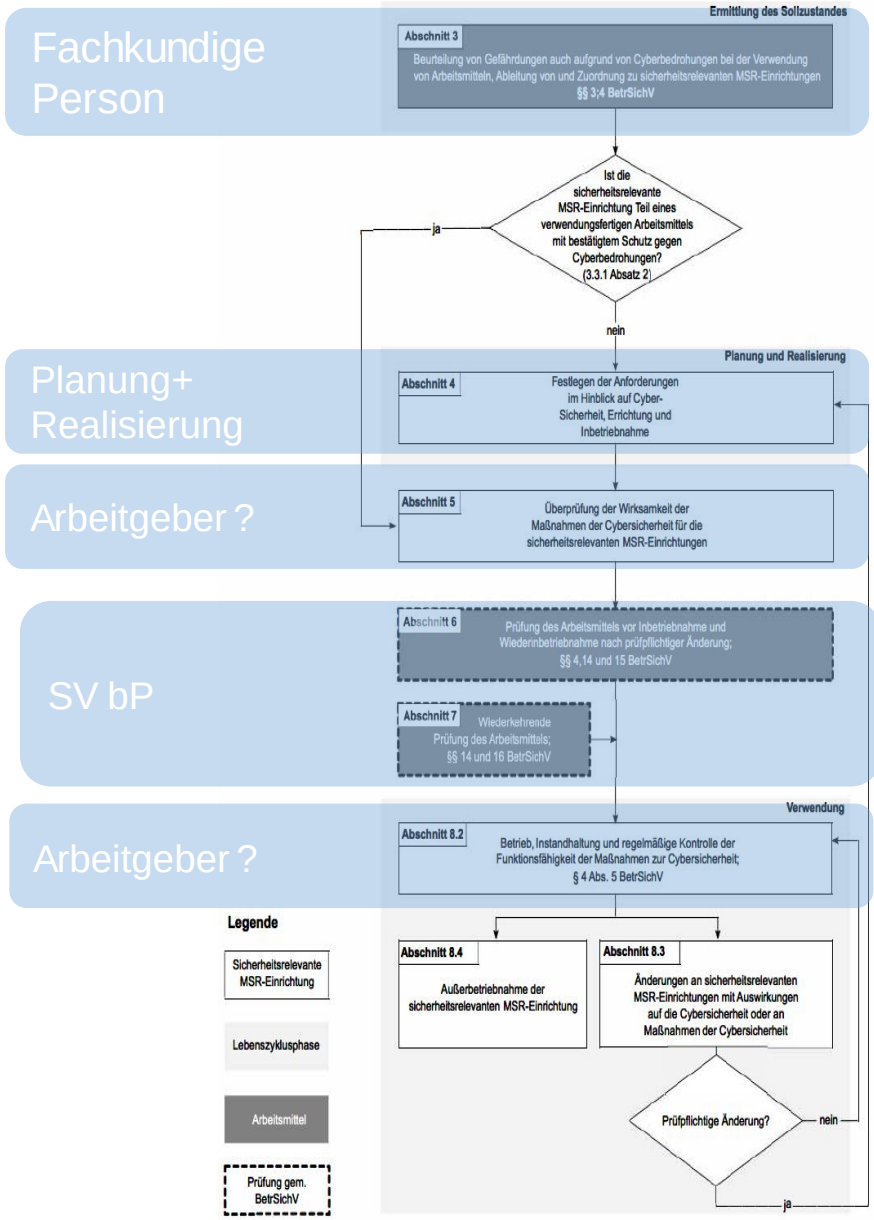
Genau das sind die Maßnahmen !!!



TÜVRheinland®
Genau. Richtig.

Agenda

Kapitel	Thema	Dauer	Referent	Seite
1	Einführung			
2	Anwendungsbereich			
3	Begriffe			
4	Anforderungen allgemein			
5	Fachkunde			
6	Wann sind Cyberbedrohungen relevant ?			
7	Anforderungen Gefährdungsbeurteilung			
8	Planung und Realisierung			
9	Überprüfung und Prüfung			



Berücksichtigung der Cybersicherheitsmaßnahmen in den Abläufen bei Planung, Realisierung und Verwendung einer sicherheitsrelevanten MSR-Einrichtung

Anforderungen Gefährdungsbeurteilung

Anforderungen Gefährdungsbeurteilung

- Die Anforderungen an die Zuverlässigkeit für sicherheitsrelevante MSR-Einrichtung wird in der GBU festgelegt.

Ziele:
Einhaltung der festgelegten Funktionsfähigkeit und Zuverlässigkeit der sicherheitsrelevanten MSR-Einrichtungen

- Für Arbeitsmittel und Anlagen mit sicherheitsrelevanten MSR-Einrichtungen sind die erforderlichen Maßnahmen der Cybersicherheit zu ermitteln und in einem Schutzkonzept der Cyber-Sicherheit zu dokumentieren.

- Die Vorgaben der Hersteller sicherheitsrelevanter MSR-Einrichtungen zur Cyber-Sicherheit (CS) sind bei der Einbindung in das Arbeitsmittel zu beachten.

Wie konkret die Gefährdungsbeurteilung zu erfolgen hat, steht nicht in dieser TRBS

Anforderungen Gefährdungsbeurteilung

IT ≠ OT ? (aber manche Sachen sind doch gleich ähnlich)

IT	Sicherheitsziel & Prioritäten	OT
mittel	Availability requirement	sehr hoch
Verzögerungen akzeptiert	Real-time requirement	kritisch
3-5 Jahre	Component lifetime	bis zu / über 20 Jahre
regelmäßig / geplant	Application of patches	bedächtig / selten
geplant / vorgeschrieben	Security testing / audit	gelegentlich
hoch / ausgereift	Security awareness	zunehmend

Anforderungen Gefährdungsbeurteilung

Besonderheiten der IT/OT-Umgebung

Kategorie	Klassische IT (office)	IT/OT-Umgebung (plant)
Performance	▪ keine garantierten Abarbeitungszeiten ▪ hohe Latenz u. U. akzeptabel	▪ garantierte Abarbeitungszeiten ▪ Latenz ist zum Teil hart begrenzt
Verfügbarkeit	▪ Rebooten von Systeme nicht ungewöhnlich ▪ Kurzfristig Wartungsvorgänge (z. B. Patch) ▪ Wartungsausfälle verursachen geringe Kosten	▪ Reboot im produktivem Umfeld nicht akzeptabel ▪ Wartungszyklen nur mit langem Vorlauf ▪ Wartungsausfälle verursachen hohe Kosten
Beurteilung von Risiken	▪ Vertraulichkeit und Integrität von Daten stehen im Vordergrund ▪ Wesentliche Risiken betreffen die nachhaltige Störung von Geschäftsprozessen	▪ Schutz von Mensch und Umwelt stehen im Vordergrund ▪ Wesentliche Risiken betreffen den unzureichenden Schutz von Menschen, Umwelt und Produktionskapazitäten.
Systemressourcen / Dediziertheit	▪ Systeme verfügen über freie Ressourcen, die beispielsweise die Installation von IT-Security-Tools auf dem System erlauben	▪ Installation von fremden Softwarekomponenten auf den Systemen nicht oder erst nach Freigabe vorgesehen, z. B. Virenschutzprogramme, Programme
Lebenszeit der Komponenten	▪ wenige Jahre	▪ bis 20 Jahren oder mehr

Anforderungen Gefährdungsbeurteilung

Identifikation Handlungsfelder Cybersicherheit (IHC)

- welche Anlagen und Standorte sind betroffen,
- wer ist verantwortlich für den Betrieb oder Produktion,
- welche Personen sind für die Gefährdungsbeurteilung und für die separate Umsetzung der Cybermaßnahmen erforderlich,
- aufgrund welcher Rechtsgebiete sind ggf. auch Maßnahmen der Cybersicherheit erforderlich,
- gibt es im Unternehmen ggf. schon Maßnahmen der Cybersicherheit, die speziell auf die Anlagen abgestimmt sind,
- sind die Schutzziele und das mögliche Schadensausmaß bekannt,
- sind die betroffenen Komponenten der OT bekannt und erfasst?

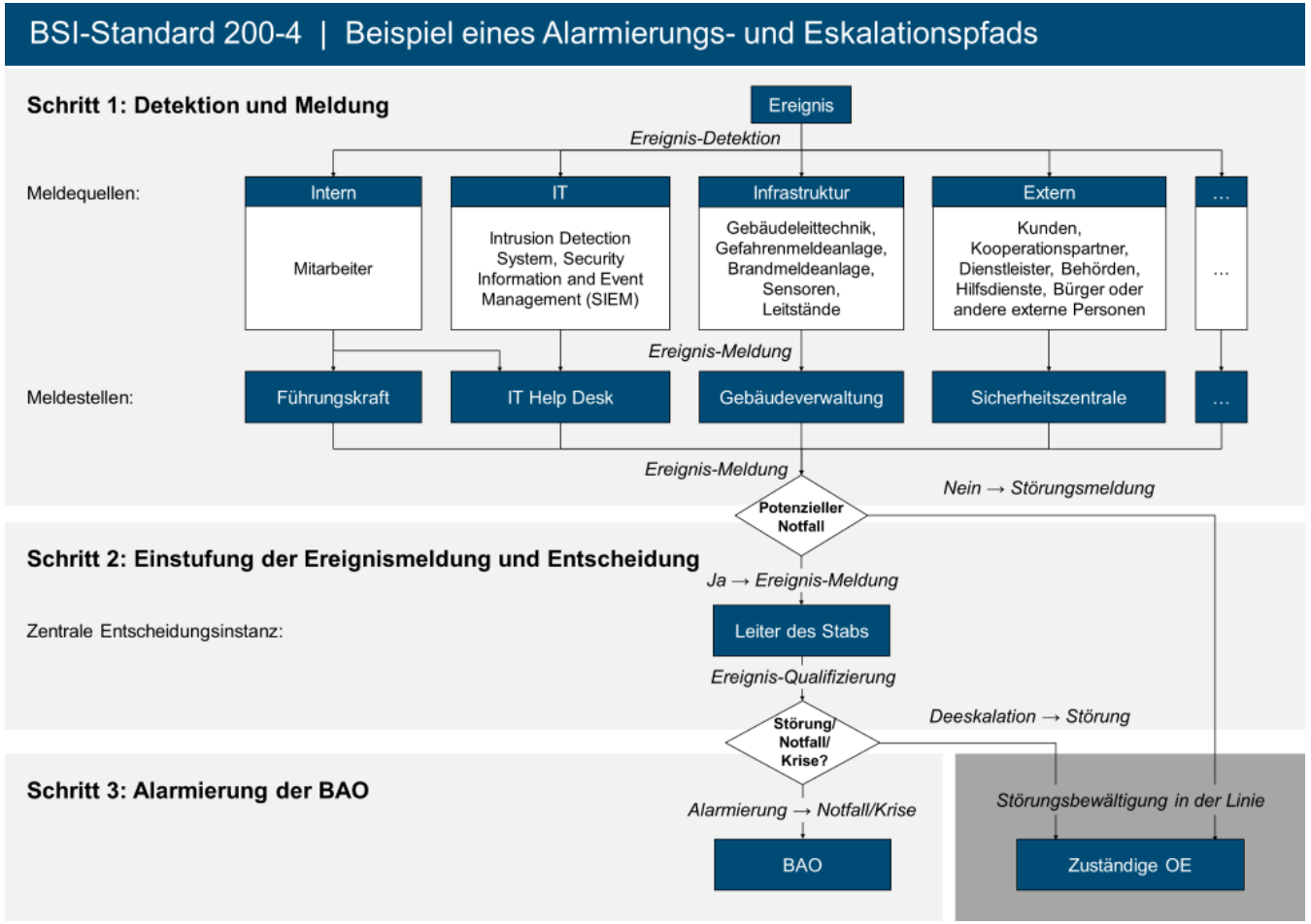
Anforderungen Gefährdungsbeurteilung

Empfehlung

- Einbindung der Fragestellungen in: HAZOP, ROGA, GBU, Sicherheitsgespräche und Explosionsschutzdokumente,
- Frage: wie kann es durch Cyberangriffe zu Situationen kommen, die eine Anlage in einen unsicheren Zustand führen?
- Beurteilung: welche Auswirkung hat eine Kompromittierung der sicherheitsrelevanten MSR?
- Festlegung der erforderlichen Cybersicherheit zur Sicherstellung der Zuverlässigkeit der MSR-Einrichtung z.B. Security – Level Target (SL-T)
- Berücksichtigung TRBS 1115-1 mit Anforderungen an die zu treffenden Maßnahmen

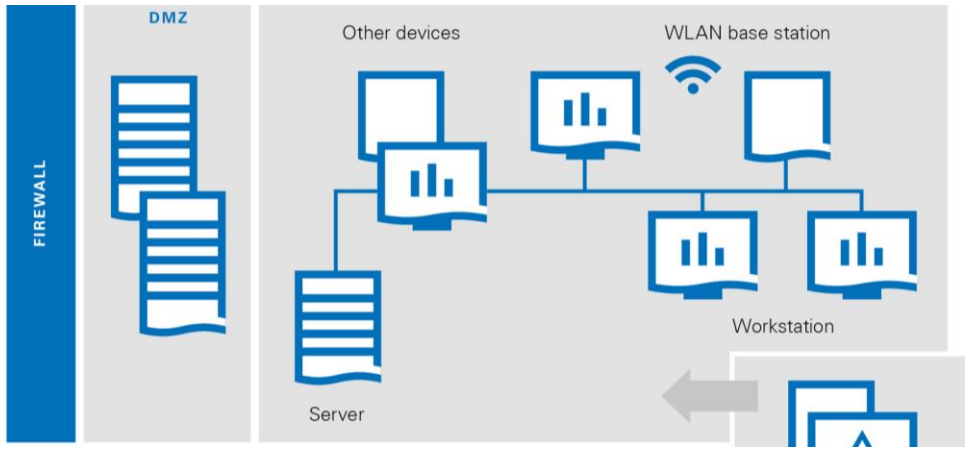
Anforderungen Gefährdungsbeurteilung

Und wenn doch mal etwas passiert



Anforderungen Gefährdungsbeurteilung

Notwendige Informationen und Unterlagen



- Schematische Darstellung der Anlage
- Netzwerkplan
- Auflistung der sicherheitsrelevanten MSR-Einrichtungen
- Funktionsbeschreibung der Anlage

Anforderungen Gefährdungsbeurteilung

Risikograph

Eintrittswahrscheinlichkeit		Auswirkung /Schadensereignis			
		leichte Verletzung einer oder mehrerer Personen	schwere irreversible Verletzung einer oder mehrerer Personen;	Tod mehrerer Personen	sehr viele Todesopfer
			Unterbrechungen möglich	Erheblicher Zeit - und Ressourcenaufwand	Erhebliche Beeinträchtigung der Betriebsabläufe
			< 1 Mio. €	(1 Mio. € - 10 Mio. €)	(> 10 Mio. €)
	Unwahrscheinlich (es ist unwahrscheinlich, dass der Angriff erfolgt)	Gering **SL-T 1**	Mittel **SL-T 2**	Mittel **SL-T 2**	Hoch **SL-T 3**
	Möglich (der Angriff wird wahrscheinlich auftreten)	Gering **SL-T 1**	Mittel **SL-T 2**	Hoch **SL-T 3**	Extrem **SL-T 4**
	Wahrscheinlich (der Angriff wird auftreten)	Mittel **SL-T 2**	Hoch **SL-T 3**	Hoch **SL-T 3**	Extrem **SL-T 4**

Individuelle Festlegung

Der Arbeitgeber / Betreiber hat die Gefährdungen / Risiken zu ermitteln, zu beurteilen und notwendige Schutzmaßnahmen abzuleiten.

Folgende Aspekte können relevant sein:

- Betrieb der Anlage (Verfügbarkeit)
- Finanzielle Auswirkungen / Umweltschäden
- Gefährdungen für Beschäftigte und andere Personen

Hieraus können Anforderungen an die Cybersicherheit abgeleitet werden

Anforderungen Gefährdungsbeurteilung

Beispiel

2.	Gefährdungsbeurteilung				
ist s MSR-Technik verbaut?	X	Ja		Nein, Beurteilung/Anlagenabschnitt endet hier.	
	Begründung:				
Kompromittierbare s MSR-Technik?	X	Ja		Nein, Beurteilung/Anlagenabschnitt endet hier.	
	Begründung:				
Verwendungsfertiges Arbeitsmittel nach 3.3.1 Absatz 2 TRBS1115-17		Ja	X	Nein	
	Begründung:				
	Im Unternehmensnetz und der angeschlossenen DMZ (HRS Connect) sind nur zum Teil verwendungsfertige Arbeitsmittel verbaut und/ oder diese verfügen augenscheinlich nicht über das erforderliche Sicherheitslevel ohne das zusätzliche techn.und org. Schutzmaßnahmen implementiert sind.				
	Die Anlage, welche durch den Hersteller XY in Verkehr gebracht wurde ist als sicher/ nicht kompromittierbar einzustufen. Folgendem Anhang aufgeführten Dokumente belegendies .Seitens der Herstellergeforderten Sicherheitsmaßnahmen wurde umgesetzt und sind im folgendenunter den Punkten 5.und im Anhangeinsehbar.				

3.	Risikobeurteilung	
3.1 Aufteilung des IACS in logisch und pyhsisch getrennte Netz/ Funktionsbereiche	Segment 1:	Anlage (egendwie muss hier ein sinnvoller Name hin)
	kompromitierbare Assets innerhalb des Segmentes	Es handelt sich lediglich um Read-Only Zugriffe. Zusätzlich im Netzsegment der Anlagenstandorte befinden sich weitere Systeme wie das Kassensystem oder ein Anlagenmonitoring, welches lesendauf die Herstelleranlage zugreifen kann. (aufführen der Komponentenaus der Assetliste)
	Segment 2:	Unternehmensnetz
	kompromitierbare Assets innerhalb des Segmentes	Router/ Firewall Hersteller XY Rechner 1 Rechner 2 Drucker 1 Smartphone 1
	Segment 3:	DMZ
	kompromitierbare Assets innerhalb des Segmentes	Server XY Firewall DB
3.2 Risikoanalyse,zu erwartende Gefährdungen, Schwachstellen	Gefährdung 1	
	Gefährdung 2	
	Gefährdung 3	
	Gefährdung 4	
	Gefährdung 5	

3.3 Wahrscheinlichkeit des Eintritts einer Cyberattacke		Auswirkung/Schwere grad				Ereignis
		leichte Verletzung von einer oder mehreren Personen	schwere irreversible Verletzungen	Todliche Verletzungen	viele Todesopfer	gesundheitliche Gefährdung
			Unterbrechungen möglich	großer Zeit- und Ressourcenaufwand	Erhebliche Beeinträchtigung der Betriebsabläufe	Betriebsstörung
		<0,5 Mio €	< 1 Mio €	<10 Mio €	> 10 Mio €	Kosten
	Nicht wahrscheinlich	Gering SL-1	Mittel SL-2	Mittel SL-2	Hoch SL-3	
	Möglich	Gering SL-1	Mittel SL-2	Hoch SL-3	Extrem SL-4	
	Wahrscheinlich	Mittel SL-2	Hoch SL-3	Hoch SL-3	Extrem SL-4	

3.4 Festlegung des Securitylevel für die Segmente nach 3.1	Folgende SL-T sollen nach IEC 62443-3-3 für das zugrunde liegende IACS erreicht werden			
	Segment 1	Tankstelle	angestrebter SL-T nach 3.2	2
	Segment 2	Leitwarte	angestrebter SL-T nach 3.2	1
	Segment 3	DMZ	angestrebter SL-T nach 3.2	2
	Segment 4		angestrebter SL-T nach 3.2	
	Segment 5		angestrebter SL-T nach 3.2	
	Begründung:			

5	Zusätzliche Anforderungen und Maßnahmen			
a) Zusätzl. geltende Anforderungen nach anderen Verordnungen, TRBS, DIN-Normen bzw. zusätzlich getroffene technische Schutzmaßnahmen	X	Sonstiges: ICS - Kompendium		
	Da nicht alle Functional Recuirements der EN 62443-3-3 umsetzbar sind, sollen zusätzlich alle Anforderungen an IACS nach Punkt 5. Best Practice Guide für Betreiber anwendung finden. (Etablierte ISO 27001:2022 Zertifizierung)			
b) Zusätzliche organisatorische Maßnahmen	x	sonstige, zusätzlich getroffene org. Schutzmaßnahme		
	- Schulungen/Unterweisung für Mitarbeiter für das verwenden von AM bzw. sMSR bzw. Computertechnik - Cyberschulungen für IT-Personal - Erstellung von Betriebsanweisungen für das Härten der Komponenten (sowohl Betreiber als auch Hersteller) - Ablage und Umsetzung der Herstellervorgaben und –unterlagen - Beschreibung von Anforderung an die fachkundigen Personen für Montage sowie Instandhaltung der sicherheitsrelevanten MSR-Einrichtungen und IT/OT - Beschreibung der benötigte Qualifikation der fachkundigen Personen zur Durchführung der Gefährdungsbeurteilung - Beschreibung und EInschränkung der Zugang und Zugriffe auf die Komponenten, Definition von Anforderungen an den Zugang/Zugriff für die Anlagenhersteller - Beschreibung und Definition von Verantwortlichkeiten für Cybersicherheitsmaßnahmen - Einführung und Dokumentation eines schlüssigen Notfallmanagementsystem - Definition von Vorgaben für Dienstleiter und Lieferanten - Erweiterung der bestehenden Ausschreibungstexte durch Inhalte der Cybersecurity - Prüfung/Ergänzung bestehender Arbeitsanweisungen hinsichtlich Aspekten der Cybersecurity		
c) Zusätzliche Maßnahmen und Anforderungen der Hersteller	Laut der Betriebsanweisung für die Wasserstofftankstelle Linde IC90 sind folgende Schutzmaßnahmen umzusetzen			
d) Prüfungen und Kontrollen nach BetrSichV / TRBS 1115-1	Prüfung nach BetrSichV und TRBS 1115-1			
		Bezeichnung	Prüffrist	Prüfung durch
	x	Prüfung des Arbeitsmittels vor Inbetriebnahme und Wiederinbetriebnahme nach prüfpflichtiger Änderung nach §§ 14 und 15 BetrSichV	-	zPbP nach BetrSichV
	x	Wiederkehrende Prüfung von Arbeitsmitteln mit sicherheitsrelevanten MSR Einrichtungen nach §§ 14 und 16 BetrSichV	1 Jahr	zPbP nach BetrSichV
	x	Funktionsfähigkeitsprüfung	3 Monate	Fachkundige Person
	x	Prüfung auf neue Cyberbedrohungen	1 Monate	zPbP nach Nummer 3.1 Anhang II der BetrSichV
	x	Änderung des Stand der Technik	1 Jahr	zPbP nach Nummer 3.1 Anhang II der BetrSichV
	Sonstige Prüfungen:			
	x	Systemtest	1 Monate	zPbP nach Nummer 3.1 Anhang II der BetrSichV

Anforderungen Gefährdungsbeurteilung

Organisatorische Gefährdungen

Gefährdung	Mögliche Maßnahmen
Unzureichende Regelung zur Cybersicherheit	▪ Klare Regelungen von Zuständigkeiten ▪ Einbeziehung von fachkundigem Personal ▪ Regelungen zu Beschaffung, Entsorgung von Komponenten ▪ Regelung Einstellung Personal und Fremdfirmen
Unzureichende Dokumentation	▪ Netzwerkpläne, Auflistung von Komponenten, Applikationen usw. ▪ Die Dokumentation gehört mit zur GBU und Integration von Maßnahmen ▪ Erforderlich für Behebung von Fehlern und Aufrechterhaltung der Stabilität
Fernzugänge	▪ Überwachung und Wartung von Prozessen aus der Ferne ▪ Einfallstor für Angreifer ▪ Zugriffe auch direkt auf Level 2 oder 3 möglich
Komponenten mit identifizierten Schwachstellen	▪ Schwachstellen sind bekannt und werden offen kommuniziert ▪ Virenschutz oder Patches oft schwierig ▪ Betroffen sind z.B. Bedien- und Engineeringsysteme
Fehlende Überwachung der IT-Umgebung	▪ Werden ungewöhnliche Ereignisse von ICS nicht oder unzureichend überwacht, so können beispielsweise Angriffsversuche oder absehbare Ausfälle nicht frühzeitig erkannt werden.
Mangelnde Awareness	▪ Die Mitarbeiter tragen stark zur Cybersicherheit in einem Unternehmen bei. Wenn diese nicht für die Bedrohungen sensibilisiert sind, bestehen erhöhte Risiken.

Zum Nachlesen

Anforderungen Gefährdungsbeurteilung

Zum Nachlesen

Vorsätzliche Handlungen / Angriffe

Gefährdung	Beschreibung
Kommunikation von Mess- und Steuerwerten	▪ Die Systeme in ICS kommunizieren untereinander über verschiedene Netzprotokolle und Technologien. Neben Ethernet, TCP/ IP, WLAN, GSM) werden ICS spezifische Protokolle eingesetzt. Diese sind überwiegend nicht unter Berücksichtigung der IT-Security entwickelt worden und bieten demzufolge keine oder nur eingeschränkte IT-Security-Mechanismen ▪ Die Integrität der Mess- und Steuerwerte ist angreifbar ▪ Auswirkungen: Verlust der Anzeige, Manipulation der Anzeige, Störung oder Verlust der Kontrolle
Brute-Force-Angriffe	▪ Einsatz automatisierte Angriffswerkzeuge, die auf unterschiedlicher Datenbasis versuchen, Kennwörter zu ermitteln ▪ Insbesondere Standardzugangsdaten und nicht ausreichend komplexe, triviale und zu kurze Passwörter können mittels dieser Angriffstechniken effizient und in kurzer Zeit ermittelt werden
Schwachstellensuche über das Netzwerk	▪ Mittels eines sogenannten Port-Scans (z.B. Nmap) lassen sich die erreichbaren Dienste über das Netz ermitteln (z. B. TCP- und UDP-Scan). Anschließend können mittels Schwachstellenscannern diese mittels hinterlegten Testvektoren auf spezifische, bekannte Schwachstellen überprüfen.
Denial-of-Service-Angriff (Dos)	▪ Diese verfolgen das Ziel, die Verfügbarkeit von Systemen oder angebotenen Diensten einzuschränken. Werden beispielsweise von einem Angreifer gezielt Ressourcen durch eine Vielzahl von gleichzeitigen Anfragen gebunden, so ist die Komponente aufgrund der Last ggf. nicht mehr für andere Nutzer erreichbar. ▪ Erfolgt die Kommunikation mittels Funk, kann ein Angreifer diese durch Überlagerungen unterbrechen

Anforderungen Gefährdungsbeurteilung

Vorsätzliche Handlungen / Angriffe

Zum Nachlesen

Gefährdung	Beschreibung
Man-in the –Middle-Angriff	▪ Der Angreifer nimmt eine Position zwischen zwei Kommunikationspartnern ein, um übertragenen Daten mitzulesen oder zu manipulieren. Dies kann physisch z. B. durch das Auftrennen einer Leitung und der direkten Verbindung zu den beiden Kommunikationspartnern geschehen oder logisch über das Vortäuschen der Identität des jeweils anderen Kommunikationspartners, sodass der Angreifer fälschlicherweise für den jeweils anderen Partner gehalten wird.
Phishing	▪ Der Angreifer gibt sich dem Benutzer als vertrauenswürdige Person oder Stelle aus (z. B. Administrator, Kollege, ICS-Hersteller). Er versucht auf diese Weise an Informationen wie Zugangsdaten zu gelangen oder den Benutzer dazu zu veranlassen, gewisse Aktionen durchzuführen (z. B. Änderung einer sicherheitsrelevanten Konfiguration, Installation eines Schadprogramms im E-Mail-Anhang). Der Angreifer versucht also, Vertrauensbeziehungen des Benutzers auszunutzen
Injection-Angriff	▪ Ein Angreifer einer Anwendung präparierte Eingabedaten und versucht damit, Befehle auszuführen. Dies betrifft im wesentlichen verarbeitende Dienste. Es beruht auf einer mangelhaften Validierung von Eingabedaten. Z.B SQL-Injection-Angriffe, bei denen einer Web-Anwendung speziell konstruierte Daten übermittelt, die einen Befehl auf der Datenbank ausführen sollen. Wenn die Daten nicht auf Plausibilität geprüft, ist eine Manipulation der Inhalte in der Datenbank möglich weil diese als Befehl interpretiert werden.
Cross-Site-Scripting (XSS-Angriff)	▪ Ein Angreifer versucht, über eine WEB-Site indirekt Schadcode (in der Regel Browser-seitig ausführbare Skripte, wie z. B. JavaScript) an den Client des Benutzers einer Web-Anwendung zu senden.

Anforderungen Gefährdungsbeurteilung

Zum Nachlesen

Vorsätzliche Handlungen / Angriffe

Gefährdung	Beschreibung
Drive-By-Downloads	▪ Durch Schwachstellen in Browsern kann allein das Betrachten einer mit Schadcode präparierten Seite zu einer Infektion des Rechners mit Schadsoftware führen. Dies wird Drive-By-Download (auch Drive-By-Exploit) genannt. Es ist hierfür keine weitere Interaktion mit dem Benutzer erforderlich.
Engineering-Workstation (EWS)	▪ Mit einer infizierten EWS , können: • Die Programme auf der SPS verändert werden. • Die Programme und Abläufe auf der SPS entwendet und an den Angreifer übertragen werden. ▪ Dieser Angriffsvektor ist besonders wertvoll, da hierdurch auch die Visualisierung des Steuerungszustands beeinflusst wird. Folge, das Bedienpersonal bemerkt die Auswirkung des Angriffs ggf. nicht. ▪ Beeinträchtigte Systeme können dann über einen langen Zeitraum sabotiert werden, ohne dass dies bemerkt wird.
Schadprogramme	▪ Schadprogramme, die eigentlich auf die Unternehmens-IT abzielen, können auch für Schäden im ICS verantwortlich sein (Kollateralschäden). Dies kann zu Abstürzen, veränderten Laufzeiten oder einer Zunahme des Netzwerkverkehrs führen, wodurch es zu Ausfällen kommt.
Replay-Angriffe	▪ Kann ein Angreifer den Netzverkehr mitschneiden (z. B. das Ausführen eines Befehls mit privilegierten Rechten) ist es möglich, durch das Wiedereinspielen dieser Daten in das Netz die mitgeschnittene Aktion unbefugt erneut auszuführen
Physischer Angriff	▪ Ein Angreifer kann eine Komponente (z. B. externer Sensor oder Aktor) physisch manipulieren, um eine Reaktion der Bedienmannschaft zu provozieren. Auf diese Weise kann ein Angreifer gewisse Aktionen wie die Durchführung von administrativen Tätigkeiten beeinflussen und dann beispielsweise für weiterführende Angriffe nutzen.

Anforderungen Gefährdungsbeurteilung

Top 10 Bedrohungen	Trend seit 2019
Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme	→
Infektion mit Schadsoftware über Internet und Intranet	↑
Menschliches Fehlverhalten und Sabotage	→
Kompromittierung von Extranet und Cloud-Komponenten	↗
Social Engineering und Phishing	→
(D)DoS Angriffe	→
Internet-verbundene Steuerungskomponenten	↗
Einbruch über Fernwartungszugänge	↗
Technisches Fehlverhalten und höhere Gewalt	→
Soft- und Hardwareschwachstellen in der Lieferkette	↑

Quelle: BSI Bericht

Agenda

Kapitel	Thema	Dauer	Referent	Seite
1	Einführung			
2	Anwendungsbereich			
3	Begriffe			
4	Anforderungen allgemein			
5	Fachkunde			
6	Wann sind Cyberbedrohungen relevant ?			
7	Anforderungen Gefährdungsbeurteilung			
8	Planung und Realisierung			
9	Überprüfung und Prüfung			

Planung und Realisierung

Ausrüstung eines Arbeitsmittels Konkretisierende Normen

Die Normenreihe der EN 62443 ist sehr umfänglich und beschreibt mögliche Vorgehensweisen zur Auswahl von Maßnahmen sehr detailliert.

Eine Hilfestellung leistet hier das Mapping des **ICS Security-Kompendiums** auf die Normenreihe EN 62443

DIN EN IEC 62443-2-1
(VDE 0802-2-1)

DIN

Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation" bekannt gegeben worden.

VDE

Vervielfältigung – auch für innerbetriebliche Zwecke – nicht gestattet.

Einsprüche bis 2020-11-04

ICS 25.040.40, 35.030, 35.240.50

Entwurf

IT-Sicherheit für industrielle Automatisierungssysteme –
Teil 2-1: Anforderungen an ein IT-Sicherheitsprogramm für IACS-Betreiber
(IEC 65/756/CDV:2019);
Deutsche und Englische Fassung prEN IEC 62443-2-1:2019

- Die EN 62443-2-1 behandelt die gleichen Themen wie das ICS Security-Kompendium des BSI
- Für die Implementierung sollte ergänzend die EN 62443-2-4 und EN 62443-3-3 herangezogen werden.

Planung und Realisierung

Konkretisierende Normen

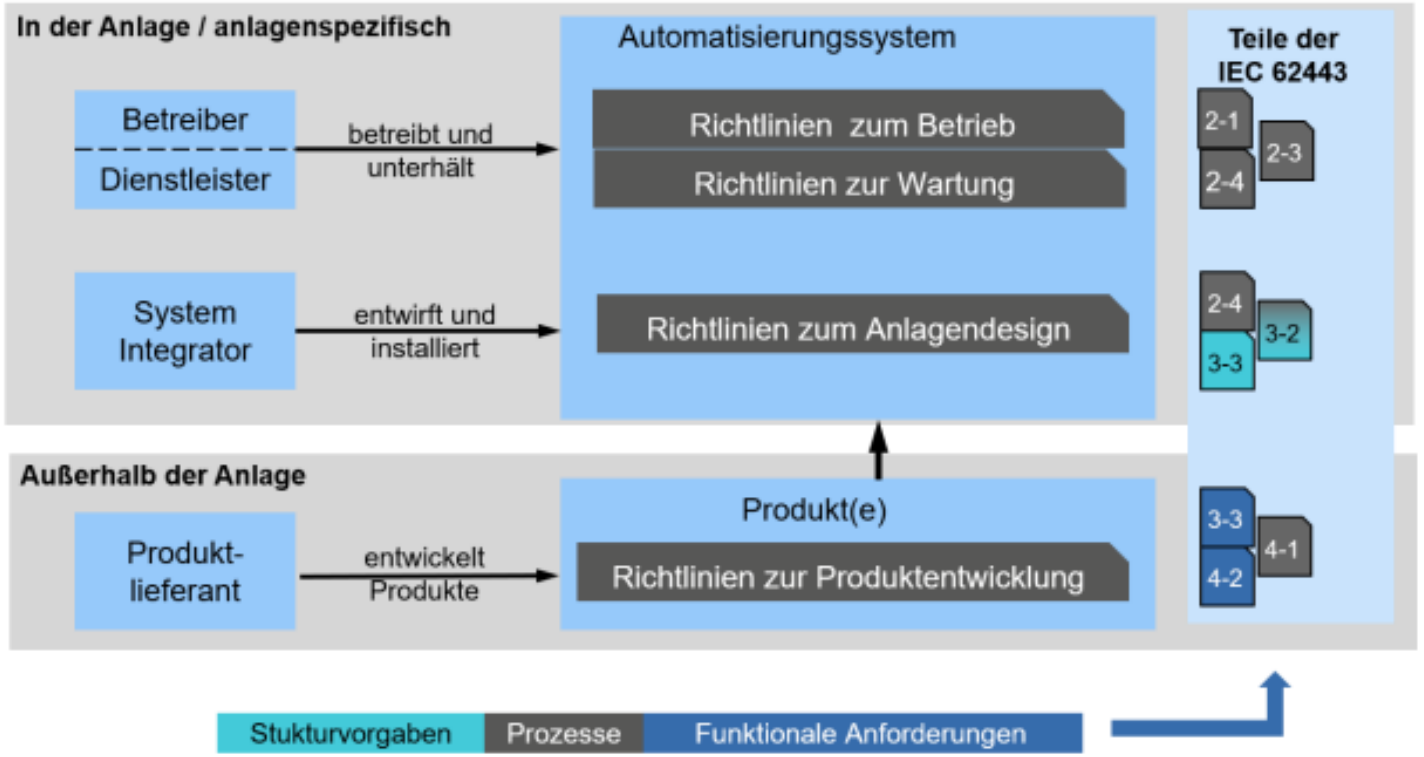


Abbildung 9: Zuordnung der ICE 62443-Normteile zu den Akteuren im Sicherheitsprozess (in Anlehnung an [ISA_62443-2-2])

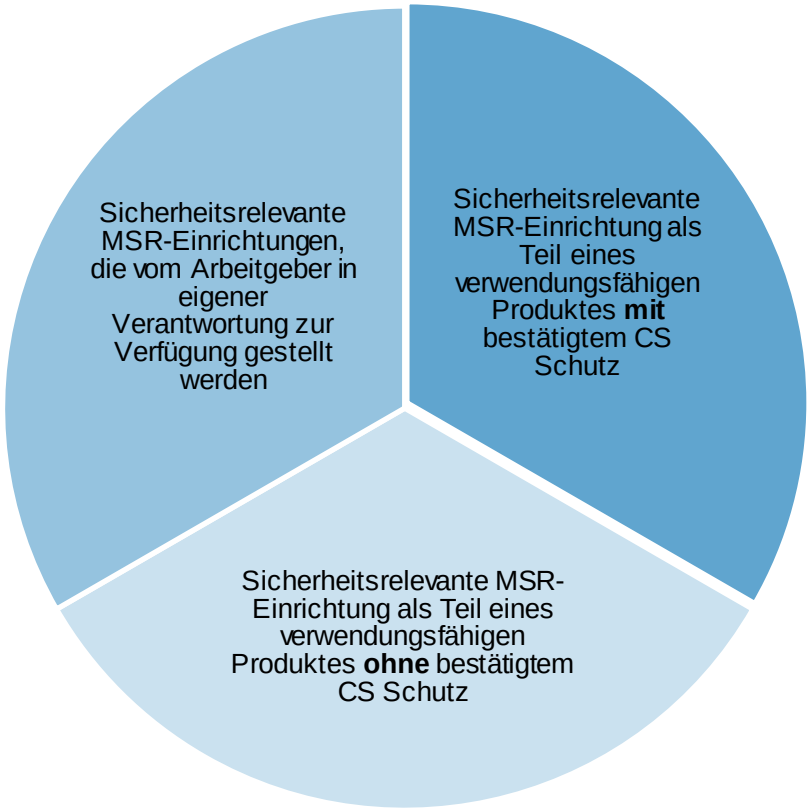
Planung und Realisierung

Konkretisierende Normen

SRs and REs		SL 1	SL 2	SL 3	SL 4
FR 5 – Restricted data flow (RDF)					
SR 5.1 – Network segmentation	9.3	→ Virtual Separation			
SR 5.1 RE 1 – Physical network segmentation	9.3.3.1	→ Physical Separation			
SR 5.1 RE 2 – Independence from non-control system networks	9.3.3.2	→ Independence of Non-control Systems			
SR 5.1 RE 3 – Logical and physical isolation of critical networks	9.3.3.3	→ Virtual and Physical Separation of Non-control Systems			
……					

Maßnahmen gegen Cyberbedrohungen

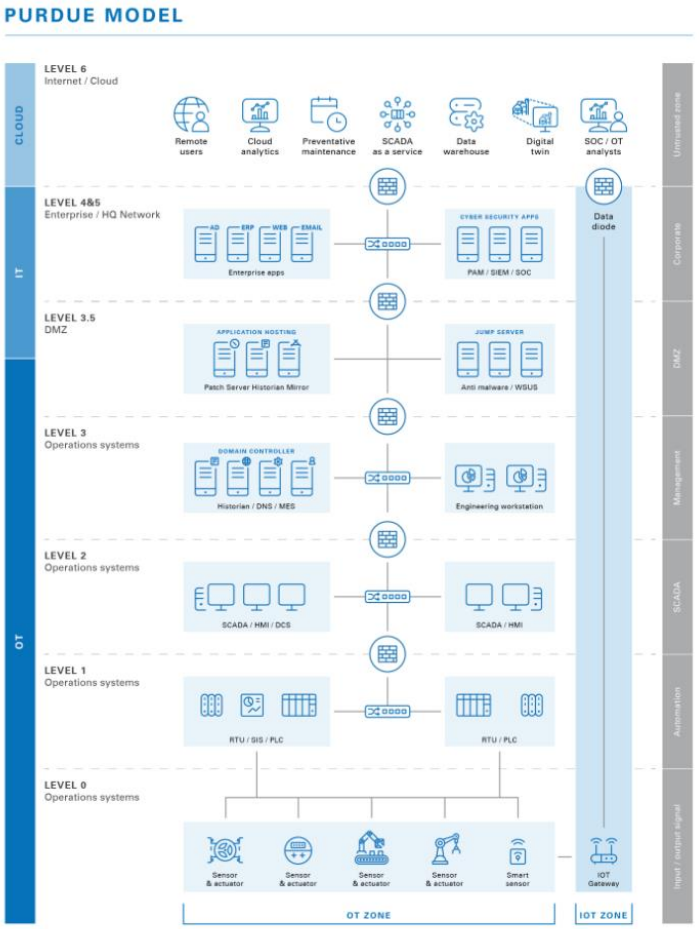
Planung und Realisierung der Ausrüstung eines Arbeitsmittels



In diesem Abschnitt werden Maßnahmen beschrieben, die der Arbeitgeber im Zuge der Planung und Realisierung sicherheitsrelevanter MSR-Einrichtungen zu treffen hat, sofern diese nicht als Bestandteil eines verwendungsfertigen Arbeitsmittels mit bestätigtem Schutz vor Cyberbedrohungen geliefert werden.

Maßnahmen gegen Cyberbedrohungen

Anforderungen für sicherheitsrelevante MSR-Einrichtungen



- Maßnahmen der Cybersicherheit ermitteln und in einem Schutzkonzept der Cyber-Sicherheit dokumentieren.
- Die Vorgaben der Hersteller sind bei der Einbindung in das Arbeitsmittel zu beachten.
- Bei der Ermittlung des Schutzkonzepts sind auch Ersatzmaßnahmen für die Zeitdauer ausgeschalteter oder eingeschränkt verfügbarer Maßnahmen der Informationssicherheit, z. B. für den Fall von Fernwartung, zu berücksichtigen.
- Die Maßnahmen der Cybersicherheit müssen geeignet sein, um die Funktionsfähigkeit der sicherheitsrelevanten MSR-Einrichtungen zu schützen, und an deren erforderliche Zuverlässigkeit angepasst sein.
- Bei Bildung von Segmenten richten sich die Maßnahmen der Cybersicherheit für das gesamte Segment nach der sicherheitsrelevanten MSR-Einrichtung mit den höchsten Anforderungen an die Cybersicherheit.

Maßnahmen gegen Cyberbedrohungen

Defense of Depth Prinzip
wird gerne mit dem Burgenprinzip erklärt.

HWI IT GmbH
Im Kreuzfeld 2
79364 Malterdingen
https://hwi-it.de/

Maßnahmen gegen Cyberbedrohungen

IDS (Intrution Detection System) Anomalie-Erkennung

Angreifer nutzen in zwei Drittel aller Fälle nur die Ports 22, 80 und 443 benutzen. Port 22 ist SSH (Secure Shell) zugewiesen, Port 80 ist HTTP (das normale unverschlüsselte Web) und 443 wird von HTTPS benutzt, dem gesicherten Webzugang.

Eine Liste der offiziell vergebenen Portnummer findet man bei der IANA.

Cyber-Sicherheit in Betriebs- und Anlagensicherheit

IDS (Intrution Detection System):

- Anschluss eines neuen Gerätes ◦
- DHCP -Requests
- Datenpakete eines bisher unbekannten Gerätes
- Datenverkehr zwischen Geräten, die bisher nicht untereinander kommuniziert haben
- Datenverkehr mit einem bisher nicht verwendeten Protokoll
- Datenverkehr mit einem unüblichen oder nicht vorgesehenen Protokoll
- Auftreten von Ereignissen zu ungewöhnlichen Zeiten
- Verwendung unerwarteter Adressen (öffentliche IP-Adressen etc.)
- allgemein auffällige Ereignisse wie Adress-Scans oder Port-Scans
- Änderungen der Netzwerkqualität wie hohe Bandbreitennutzung, Erhöhung der RoundTrip-Zeiten, Verringerung der TCP-Fenstergröße, etc.

Maßnahmen gegen Cyberbedrohungen

Vorgehensweise

! Wichtig !
Eine ganzheitliche Betrachtung ist erforderlich

1. Erfassung aller Elemente der sicherheitsrelevanten MSR-Einrichtungen und der IT/OT-Umgebung
2. Erfassung und Bewertung von Bedrohungen der Integrität und Verfügbarkeit der sicherheitsrelevanten MSR-Einrichtungen, die durch Cyberbedrohung dieser Elemente ausgehen.
3. Auswahl und Umsetzung von Cybersicherheitsmaßnahmen. Auf die erforderliche Rückwirkungsfreiheit ist zu achten.
4. Festlegungen der einzuhaltenden Fristen oder Anlässe für die Durchführung von Aktualisierungen (z. B. Updates der Virensignaturen) und Kontrollen.
5. Festlegung eines Vorgehens zur regelmäßigen Ermittlung von Schwachstellen in der IT/OT-Umgebung und den Cyberbedrohungen.

Agenda

Kapitel	Thema	Dauer	Referent	Seite
1	Einführung			
2	Anwendungsbereich			
3	Begriffe			
4	Anforderungen allgemein			
5	Fachkunde			
6	Wann sind Cyberbedrohungen relevant ?			
7	Anforderungen Gefährdungsbeurteilung			
8	Planung und Realisierung			
9	Überprüfung und Prüfung			

Überprüfung und Prüfung

Überprüfung der Wirksamkeit der Cybersicherheitsmaßnahmen

Bei der Überprüfung der Wirksamkeit der Cybersicherheitsmaßnahmen insbesondere folgende Punkte relevant:.

1. Die Spezifikationen der Cybersicherheitsmaßnahmen den Anforderungen der Gefährdungsbeurteilung entsprechen.
2. Alle Cybersicherheitskomponenten müssen funktionsfähig sein.
3. Die Beurteilungskriterien zur Bewertung der Cybersicherheitsmaßnahmen müssen eindeutig festgelegt sein.
4. Für die Überprüfung sind mindestens festzulegen:
   a) die zu den Sicherheitsfunktionen gehörenden Cybersicherheitsmaßnahmen sowie die Fristen ihrer Kontrollen,
   b) Art und Umfang der Überprüfung.

Wenig konkret

Überprüfung und Prüfung

Überprüfung der Wirksamkeit der Cybersicherheitsmaßnahmen

Was ist nun zu überprüfen?

Die Eignung und Funktionsfähigkeit der in Abschnitt 4 und GBU festgelegten Maßnahmen!

Eine Überprüfung der Wirksamkeit der Cybersicherheitsmaßnahmen vor erstmaliger Verwendung ist nicht erforderlich, wenn diese im Rahmen von §§ 14 oder 15 BetrSichV geprüft werden. Also durch die ZÜS oder bP.

Überprüfung und Prüfung

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

Prüfung der Eignung und Funktionsfähigkeit:

- Gibt es eine GBU mit Betrachtung der Cyberbedrohungen?
- Wurde ein angemessenes Maß zur Cyber-Sicherheit festgelegt? (z.B. SL-T)
- Maßnahmen sowie die Fristen ihrer Kontrollen
- Sind die Maßnahmen geeignet, wurde z.B. eine Norm zur Umsetzung herangezogen? (z.B. IEC 62443, IEC 27001 …)
- Wurden Festlegungen zu Art und Umfang der Überprüfung getroffen.
- Liegt eine Dokumentation zur Überprüfung der Wirksamkeit der Maßnahmen der Cybersicherheit nach Abschnitt 5 vor?
- Ist ein Verfahren vorhanden, das bei der Festlegung der Maßnahmen der Informationssicherheit anlassbezogen neue Erkenntnisse berücksichtigt, die z. B. aus Cyber-Sicherheitsvorfällen oder dem fortschreitenden Stand der Cybersicherheitstechnik hervorgehen.
- Liegen aktuelle Unterweisungen der Beschäftigten entsprechend vor?

Überprüfung und Prüfung

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

- Sind Vorgaben zur regelmäßigen Kontrolle der Funktionsfähigkeit vorhanden (Abschnitt 8)?

  Feststellung:

  a. ob die Maßnahmen weiterhin geeignet und funktionsfähig sind.

  b. wurden Änderungen hinsichtlich der Prüfpflicht bewertet,

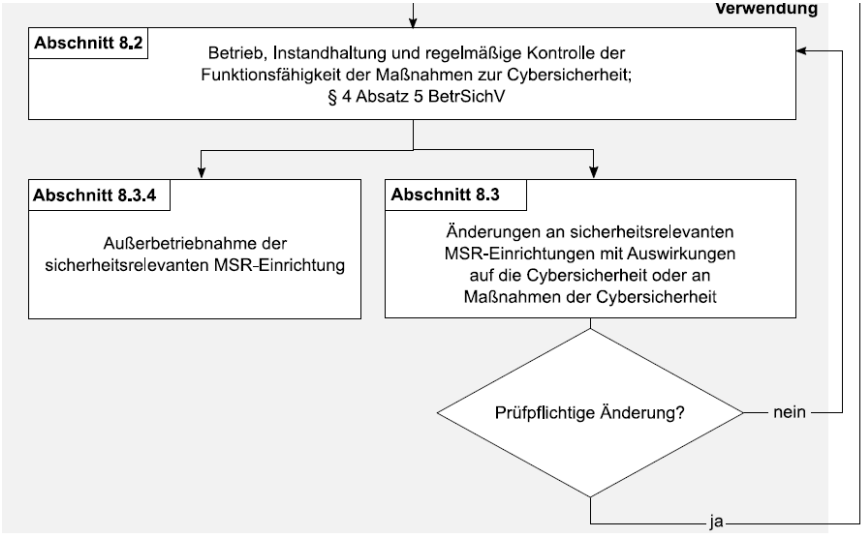
  c. wurden Änderungen an den Maßnahmen der Cybersicherheit hinsichtlich möglicher Auswirkungen auf die sMSR bewertet und

  d. wurden anlassbezogene neue Erkenntnisse zu Cyberbedrohungen, berücksichtigt, und ggf. Anpassungen vorgenommen.

- Wird die geforderte Eignung und Funktionsfähigkeit der Maßnahmen weiterhin erreicht oder ist ein Management der Cybersicherheit vorhanden

Überprüfung und Prüfung

Prüfpflichtige Änderung



Anforderungen bei prüfpflichtigen Änderung:

- zu ermitteln ob Cybersicherheitsmaßnahmen neu festzulegen sind,
- ihre Auswirkungen auf den Schutz der sicherheitsrelevanten MSR-Einrichtungen sowie deren Rückwirkungsfreiheit zu bewerten und
- die geänderten Teile zu prüfen.

Keine prüfpflichtige Änderungen sind z.B.:

- Parameteränderungen,
- Updates,
- funktionsidentischer Austausch von Komponenten,

Aber eine Änderung

Änderungen an Cybersicherheitsmaßnahmen sind zu dokumentieren und eine Kontrolle der Funktionsfähigkeit durchzuführen.

Danke für Ihre Aufmerksamkeit

TRBS 1115-1

TÜV Rheinland Industrie Service GmbH
Herr Ralf Schmitt
Am Grauen Stein
51105 Köln

Mobiltelefon 0171-9918823
ralf.schmitt@de.tuv.com

TÜVRheinland®
Genau. Richtig.