Cybersecurity auf dem Prüfstand: EU NIS2 Richtlinie & EU Cyber Resilience Act - was als Unternehmen zu beachten ist

Florian Kiel
Functional Safety & Cybersecurity & Explosion Protection

TÜVRheinland®
Precisely Right.

Warum ist ein Budget für Cybersecurity sinnvoll?

Zentrale Erkenntnisse des Bundeslagebilds Cybercrime 2023

- Straftaten im Bereich Cybercrime liegen in Deutschland weiter auf einem hohen Niveau. Das zeigt sich insbesondere mit Blick auf Cyberstraftaten, die zu Schäden in Deutschland führen, jedoch aus dem Ausland oder von einem unbekannten Ort aus verübt werden. Die Zahl dieser sogenannten Auslandstaten steigt seit ihrer Erfassung im Jahr 2020 kontinuierlich an – 2023 um 28% gegenüber dem Vorjahr. Die Zahl der Auslandstaten im Phänomenbereich Cybercrime übersteigen damit erneut die der Inlandstaten, also jene Cyberstraftaten, bei denen Deutschland gleichermaßen Handlungs- und Schadensort ist. Die Inlandstaten stagnieren auf hohem Niveau (134.407 Fälle bzw. -1,8% gegenüber 2022).
- Cybercrime richtet jedes Jahr einen hohen wirtschaftlichen Schaden an. Laut Erhebung des Branchenverbandes Bitkom e. V. lagen die im Jahr 2023 direkt durch Cyber-Angriffe verursachten gesamtwirtschaftlichen Schäden bei 148 Milliarden Euro.
- Die Aufklärungsquote bei den Cybercrime-Delikten ist 2023 um drei Prozentpunkte angestiegen und liegt nun bei 32,2 Prozent.

Quelle: BKA - Im Fokus: Bundeslagebild Cybercrime 2023 - Im Fokus: Bundeslagebild Cybercrime 2023

Regulierungen

Immer mehr Unternehmen müssen immer weitergehende Cybersecurity Anforderungen erfüllen

KRITIS

- Die KRITIS-Regulierung verpflichtet Betreiber Kritischer Infrastrukturen in Deutschland mit dem IT-Sicherheitsgesetz zu Cyber Security in KRITIS-Anlagen. Damit soll die Versorgung der Gesellschaft und Wirtschaft in den KRITIS-Sektoren in Deutschland durch Cyber Security geschützt werden
- Erweiterung der Regulierung in 2023 und 2024 erwartet

IT-Sicherheitsgesetz 2.0

- Das IT-Sicherheitsgesetz 2.0 ist seit Mai 2021 in Kraft. Es erweitert die deutsche KRITIS-Regulierung von 2015 deutlich – mehr Pflichten, größerer Betreiberkreis, höheren, mehr Befugnissen für den Staat und Regulierungsbehörden

NIS2/CRA

- Erweiterung der bisherigen Regulierung auf europäischer Ebene die bis Oktober 2024 in nationales Recht überführt werden müssen.
- Reguliert die Informationssicherheit und Resilienz von kritischen Betreibern, um die Auswirkungen von Cyber Angriffen und Störungen auf IT-Systeme und Netzwerke zu minimieren.

Branchenspezifische Regulierung

- Branchenspezifische Regulierungen für bspw.: Energie, Telekommunikation, Transport, etc.

BetrSichV

- Erweitert Pflichten im Rahmen der Betriebssicherheitsverordnung (BetrSichV) bzgl. Gefährdungsbeurteilung im Hinblick auf die sichere Verwendung von Arbeitsmitteln
- Betreiber von überwachungsbedürftigen Anlagen wie Aufzüge, Druck- oder Ex-Anlagen müssen künftig Cyber Security berücksichtigen. Gefährdungen durch Sicherheitslücken bei der Software sowie Mess-, Steuer- und Regeltechnik (MSR) gehören gemäß den aktualisierten Vorschriften der Betriebssicherheitsverordnung zum Prüfumfang der Zugelassenen Überwachungsstellen (ZÜS)

Alleine IT-SIG2 und NIS2 stellen eine Herausforderung dar. Unternehmen und Organisationen in relevanten Sektoren mit >50 Mitarbeitern und >10 Mio. EUR Umsatz sind kritisch und müssen reguliert werden.

NIS2 Sanktionsregelung: „Die NIS-Richtlinie legt eine finanzielle Obergrenze für Sanktionen in Höhe von 150.000 Euro fest, während NIS 2 eine völlig andere Größenordnung vorsieht, nämlich 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes.“

TÜVRheinland®
Genau. Richtig.

Umgebungen

OT- und IT-Systeme: unterschiedliche Betriebsanforderungen und Fähigkeiten auf Bedrohungen zu reagieren

OT		IT
Begrenzte Datenkapazität und Rechenleistung	● ◄····► ●	Hohe Datenkapazität und Rechenleistung
Safety Operations ist essentiel	● ◄····► ●	Wenige sicherheitskritische Operationen
Häufig unklare bzgl. Verantworltichkeiten zwischen Betriebsleitung/IT/Anlagenbauer	● ◄····► ●	Klare Verantwortung der IT – auch innerhalb der IT meist klar geregelt
Lange Lebensdauer führt zu veralteter, nicht unterstützter Infrastruktur	● ◄····► ●	Kontinuierliche Geräteaufrüstung mit kurzen Lebenszyklen
Langsame Reaktionen auf Bedrohungen – schnelles Patchen ist aufgrund von Ausfällen möglicherweise nicht möglich	● ◄····► ●	Schnelle Reaktion auf Bedrohungen, Patches und Neustarts sind akzeptabel

◄····· **Verfügbarkeit** ····· **Integrität** ····· **Vertraulichkeit** ·····►

TÜVRheinland®
Genau. Richtig.

Entwicklungen

Handlungsbedarf aufgrund zahlreicher Faktoren: Mangel an Fachkräften, unausgereifte Technik, fortschrittliche Sicherheitsanalysen und neue/wachsende Regulierung

DIGITALISIERUNG DER INDUSTRIE

Vernetzung	Effizienz und Dateneinsicht durch Vernetzung (z.B. Remote-Zugänge, Notfallschalter, Big Data, Analytics)
Zunehmende anspruchsvollere Cyber-Angriffe	Stetig steigende Anzahl, wachsende Ausgereiftheit und größere Auswirkungen von Cybersicherheitsangriffen. Mit Bedrohungen und Angriffen Schritt zu halten, wird ohne professionelle Hilfe unmöglich sein.
Weltweiter Mangel an (industriellen-) Cybersicherheits-fachkräften	Die Nachfrage nach Cybersicherheit insbesondere Industrial Security wird weiter ansteigen. Die Suche nach qualifizierten Ressourcen wird ohne externe Hilfe unmöglich sein.
Zunehmende Akzeptanz von Managed Security Services	Der Mangel an qualifizierten Ressourcen zwingt Unternehmen Lösungen für die Cybersicherheit auszulagern. (z.B. Managed OT SOC, Managed Threat Detection, Managed Testing)
Kritische und industrielle Infrastrukturen sind gefährdete Ziele	Die Bedrohungen zielen auf Schäden an kritischen Infrastrukturen und Diebstahl sensibler Daten ab. Besonders kritisch sind hierbei Safety-Aspekte, die Schäden an der Umwelt und dem Leib und Leben verursachen können.
Regulatorik und Gesetzgebung als Treiber	KRITIS, BetrSichV, Lieferkettensorgfaltspflichtengesetz (LkSG), ESG, branchenspezifische Gesetze, etc. zwingen Unternehmen dazu, sich um die OT Security zu kümmern.

OT Security wird getrieben von vielfältigen Innovationen und gleichsam gehemmt durch die wachsenden Bedrohungen durch Cyberkriminalität.

TÜVRheinland®
Genau. Richtig.

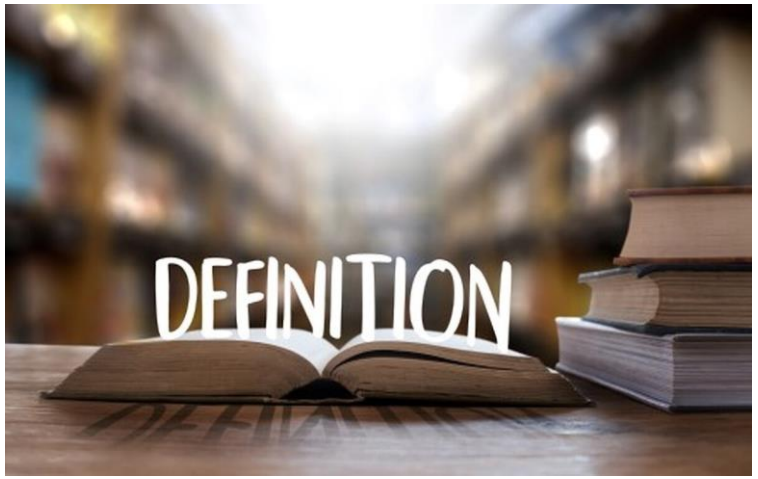
EU Richtlinie NIS-2

TÜVRheinland®
Genau. Richtig.

EU NIS-2 Definition.

Worum geht es in der EU Richtlinie NIS-2 überhaupt?

Unternehmen/
Betreiber



- "Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union„
- Ziel: Cybersicherheit in der Europäischen Union stärken
  - Hohes Sicherheitsniveaus von Netz- und Informationssystemen (NIS) in der EU
  - Verbesserung der Zusammenarbeit zwischen Mitgliedstaaten bzgl. Cybersicherheit
  - Förderung der Resilienz von kritischen Infrastrukturen und digitalen Diensten
  - Erhöhung der Fähigkeit bzgl. Reaktion auf/Bewältigung von Cybersicherheitsvorfällen
- Hauptmerkmale sind u.a.
  - Geltungsbereich: Betreiber kritischer Infrastrukturen und Anbieter wesentlicher Dienste
  - Mindestanforderungen an Cybersicherheitsmaßnahmen
  - Meldepflicht für Sicherheitsvorfälle
  - Mitgliedstaaten müssen eng kooperieren und nationale Behörden benennen

EU Richtlinie NIS-2. Betroffene Unternehmen.

„Ist mein Unternehmen von der EU Richtlinie NIS-2 betroffen?“

- Die betroffenen Unternehmen sind (indirekt) in Artikel 2 der NIS-2 Richtlinie definiert, u.a.
  - kritische Einrichtungen nach Richtlinie (EU) 2022/2557
  - mittlere Unternehmen nach Empfehlung 2003/361/EG
  - Unternehmen beliebiger Größe, die bestimmte – teilweise final noch zu definierende – Leistungen erbringen
  - Mitgliedstaaten können weiter definieren.

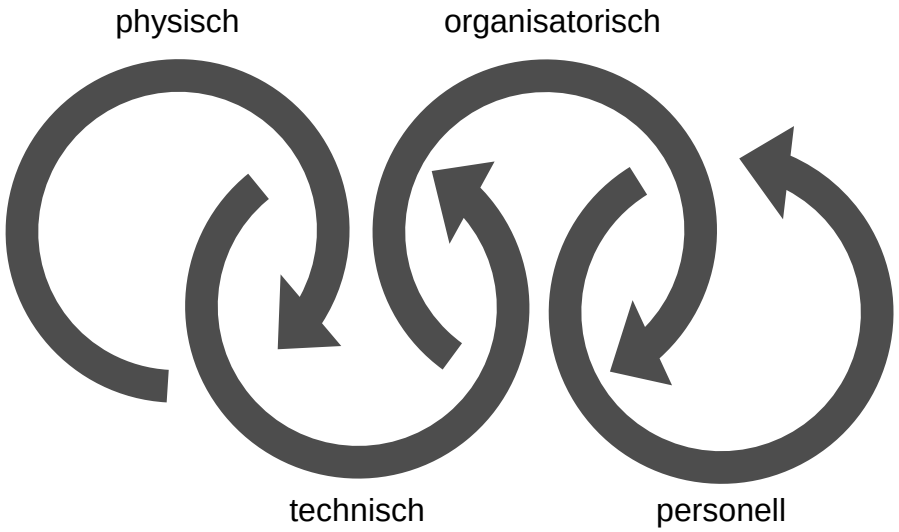
- Unternehmen aus folgenden betroffene Sektoren
  - öffentliche oder private Einrichtungen aus definierten Sektoren mit hoher Kritikalität
  - öffentliche oder private Einrichtungen aus definierten sonstigen kritischen Sektoren

- Bestimmen Sie, ob ihr Unternehmen betroffen ist
  - Unter Beiziehen ihrer Rechtsabteilung und/oder externen Juristen
  - Zeitnah auf Basis der EU Richtlinie NIS-2
  - …spätestens ab 17.10.2024 mit der nationalen Gesetzgebung

TÜVRheinland®
Genau. Richtig.

Was die EU Richtlinie NIS-2 fordert. Maßnahmen.

Welche Maßnahmen muss ein Unternehmen aufgrund der EU Richtlinie NIS-2 umsetzen?



- Recht allgemeine Forderungen
  - Konzepte/Verfahren für Einsatz von Kryptografie und gegebenenfalls Verschlüsselung
  - Maßnahmen müssen verhältnismäßig sein (Kosten, Risikorelevanz)
  - Maßnahmen müssen Stand der Technik (Normen und Standards) berücksichtigen
- Technische Maßnehmen umfassen insb.
  - Netzwerk- und Systemüberwachung, Zugriffskontrolle
  - Verschlüsselung, Schwachstellenmanagement
- Organisatorische Maßnehmen umfassen insb.
  - Sicherheitsrichtlinien, Lieferantenmanagement
  - Sensibilisierung, Schulung, Notfallplanung
  - … kontinuierliche Verbesserung

TÜVRheinland®
Genau. Richtig.

ISMS nach ISO/IEC 27001. Das Mittel der Wahl zur NIS-2 Umsetzung.

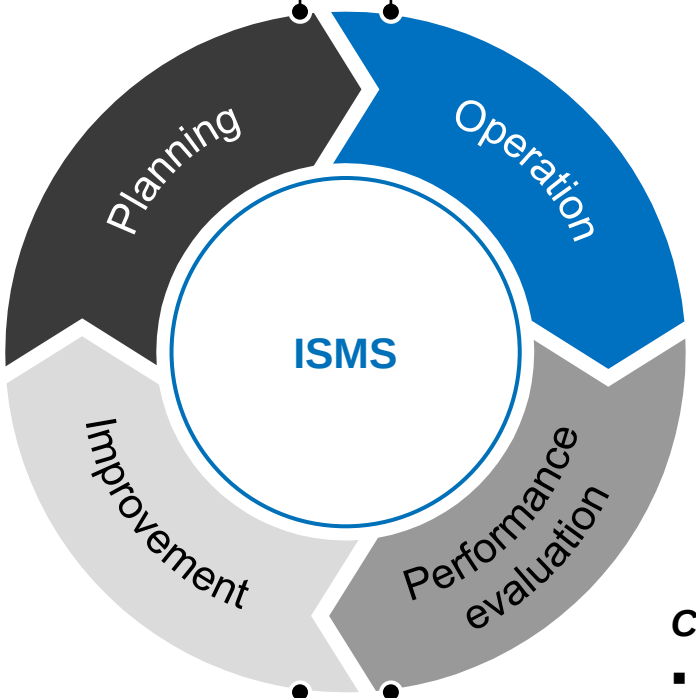
Bauen Sie ein ISMS auf und setzen Sie damit die Anforderungen der NIS-2 nachhaltig um.

PLAN

- Definition von Anwendungs-bereich und Zielen
- Risikoanalyse
- Risikobehandlung
- Maßnahmendefinition
- Ziele & Plan

DO

- Implementierung und Betrieb von Maßnahmen/Prozessen



- ISO/IEC 27001:2022
- Ggf. Spezialanforderungen berücksichtigen – z.B. IT-Sicherheitskatalog BNetzA, KRITIS oder ISO 27701 (Datenschutz)

ACT

- Behandeln von Abweichungen
- Beseitigen der Ursachen von Abweichungen

CHECK

- Messen, Analyse und Bewertung
- Interne Audits
- Management Bewertung

TÜVRheinland®
Genau. Richtig.

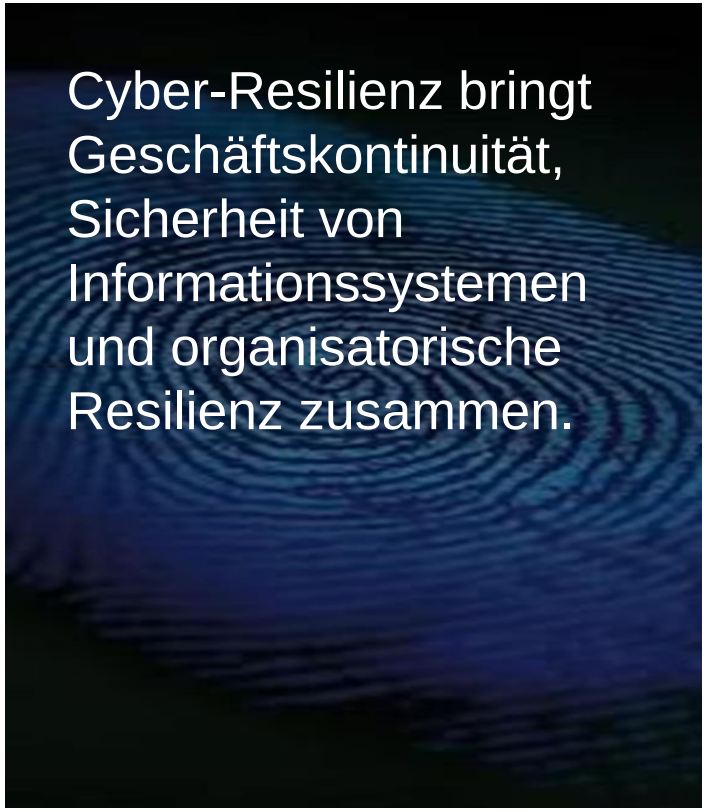
EU Cyber Resilience Act

TÜVRheinland®
Genau. Richtig.

Cyber Resilience Act

Wachsende Sicherheitsanforderungen an Produkte mit digitalen Komponenten

Hersteller/
Produkte



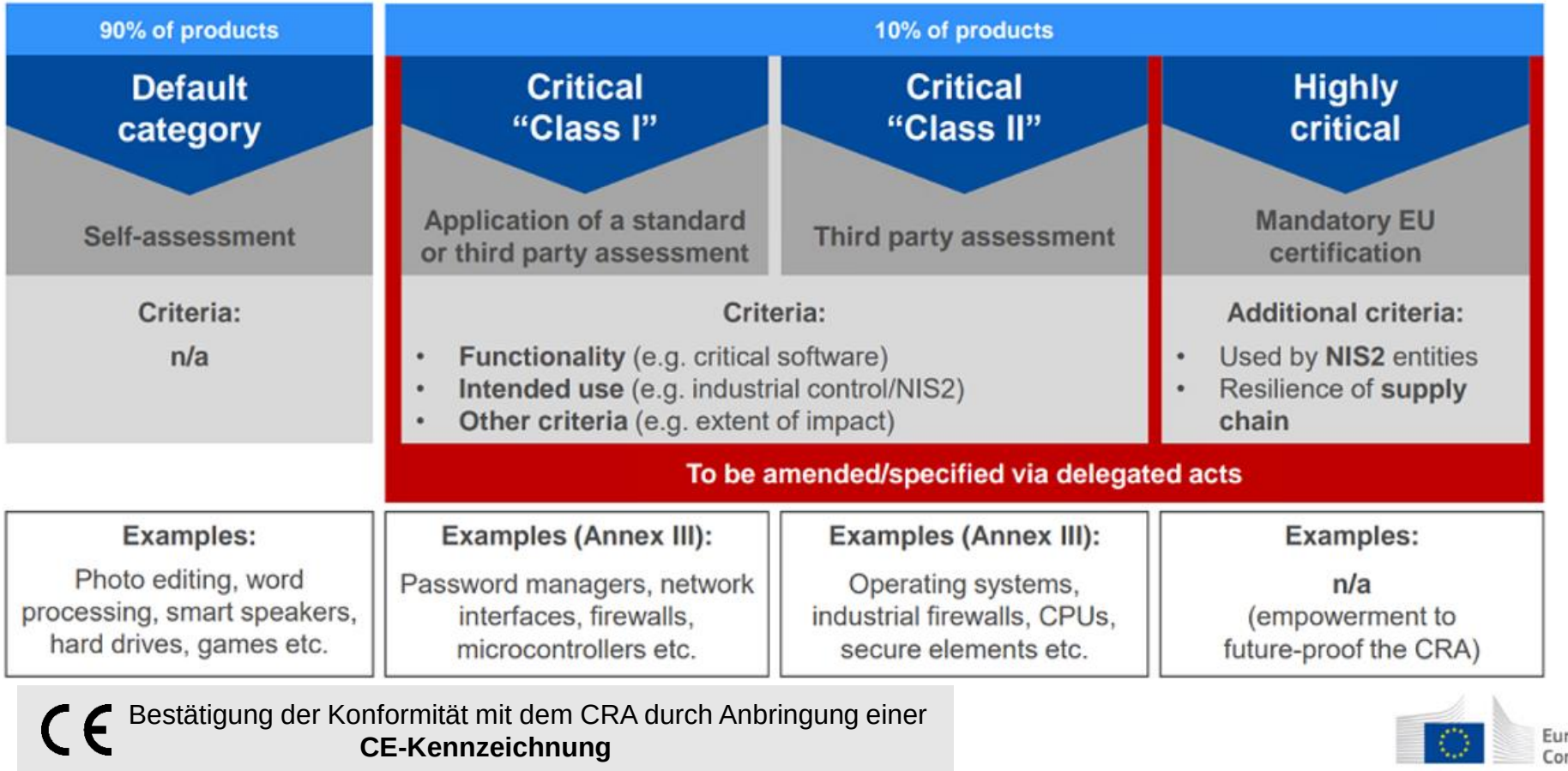
- EU Gesetzesinitiative zur Einführung des **Cyber Resilience Act** soll EU-weit Hersteller und Händler zwingen, künftig nur noch IT-Produkte mit hohen Standards für Cybersicherheit auf den Markt zu bringen.
- Ziel der EU: sicherstellen, dass Schwachstellen bei digitalen Produkten, die innerhalb der EU in den Verkehr gebracht werden, auf ein Minimum reduziert werden.
- Während des gesamten Lebenszyklus eines Produktes soll die Verantwortung der Hersteller für die Cybersicherheit ihres Produkts nicht enden.
- Verbraucher sollen darüber hinaus transparent über mögliche Sicherheitsrisiken informiert werden.
- Verstöße gegen den Cyber Resilience Act können mit hohen Bußgeldern belegt werden, (bis zu 15 Mio. Euro oder 2,5 % des weltweiten Umsatzes des vorangegangenen Geschäftsjahrs umfassen können. Die Marktaufsichtbehörden sind befugt u.a. Produktrückrufe anordnen.

! Um diese Ziele zu erreichen, benötigen wir **Security by Design**!

TÜVRheinland®
Genau. Richtig.

Cyber Resilience Act

Welche Produkte sind betroffen?



CE Bestätigung der Konformität mit dem CRA durch Anbringung einer **CE-Kennzeichnung**

European Commission

! Nicht enthalten: Open Source Software, Medical, Automotive, Aviation, Machinery...

TÜVRheinland®
Genau. Richtig.

Ein mögliches Mittel zur Erfüllung des CRA…

IEC 62443 Normenreihe

General	**IEC-62443-1-1** Terminology, concepts and models	**IEC-62443-1-2** Master glossary of terms and abbreviations	**IEC-62443-1-3** System security compliance metrics		
Policies and procedures	**IEC-62443-2-1** Establishing an industrial automation and control system security program	**IEC-62443-2-2** Implementation guidance for an IACS security management system	**IEC-62443-2-3** Patch management in the IACS environment	**IEC-62443-2-4** Security program requirements for IACS service providers	BETREIBER
System	**IEC-62443-3-1** Security technologies for industrial automation and control systems	**IEC-62443-3-2** Security risk assessment and system design	**IEC-62443-3-3** System security requirements and security levels		SERVICE PROVIDER
Component	**IEC-62443-4-1** Product development requirements	**IEC-62443-4-2** Technical security requirements for IACS components			HERSTELLER

TÜVRheinland®
Genau. Richtig.

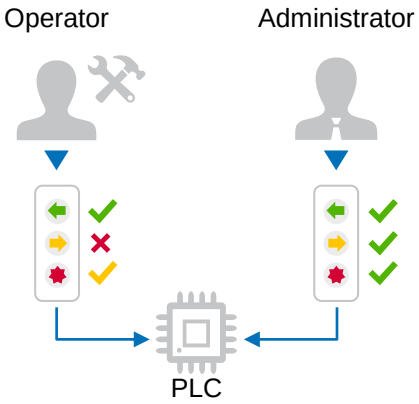
Cyber Security Anforderungen.

Grundlegende Anforderungen an die Produktentwicklung nach IEC 62443.

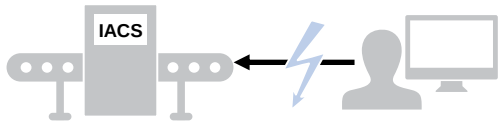
FR 7 – Ressourcen Verfügbarkeit

FR 1 – Identifikations- und Authentifizierungskontrolle

FR 2 – Verwendungskontrolle



FR 6 – Rechtzeitige Reaktion auf Ereignisse



FR 5 – Eingeschränkter Datenfluss

FR 4 – Geheimhaltung von Daten

FR 3 – System Integrität

! Um diese Ziele zu erreichen, benötigen wir **Security by Design**!

TÜVRheinland®
Genau. Richtig.

Definition von Security Leveln (SL)

IEC 62443-3-3, A 3.2

SL 0: Keine besonderen Anforderungen oder Security-Maßnahmen nötig

SL 1: Schutz gegen beiläufige oder zufällige Verstöße

SL 2: Schutz gegen gezielte Verstöße, ausgeübt mit einfachen Mitteln, mit geringen Ressourcen, allgemeinen Fähigkeiten und geringer Motivation

SL 3: Schutz gegen gezielte Verstöße, ausgeübt mit technisch ausgereiften Mitteln, mit moderaten Ressourcen, IACS spezifischen Fähigkeiten und moderater Motivation

SL 4: Schutz gegen gezielte Verstöße, ausgeübt mit technisch ausgereiften Mitteln, mit erheblichen Ressourcen, IACS spezifischen Fähigkeiten und hoher Motivation

…ein Beispiel für den Stand der Technik

Generischer Standard für funktionale Sicherheit: IEC 61508:2010

1 FUNKTIONALE SICHERHEIT

2 CYBERSECURITY

Fachgrundnorm für funktionale Sicherheit: IEC 61508:2010

7.4.2.3

„… Wenn die Gefährdungsanalyse feststellt, dass eine böswillige oder nicht autorisierte Handlung ….. als vernünftigerweise vorhersehbar gilt, sollte eine Bedrohungsanalyse … durchgeführt werden.

ANMERKUNG 3 Für eine Anleitung zur Risikoanalyse …. Siehe **Normenreihe IEC 62443.**

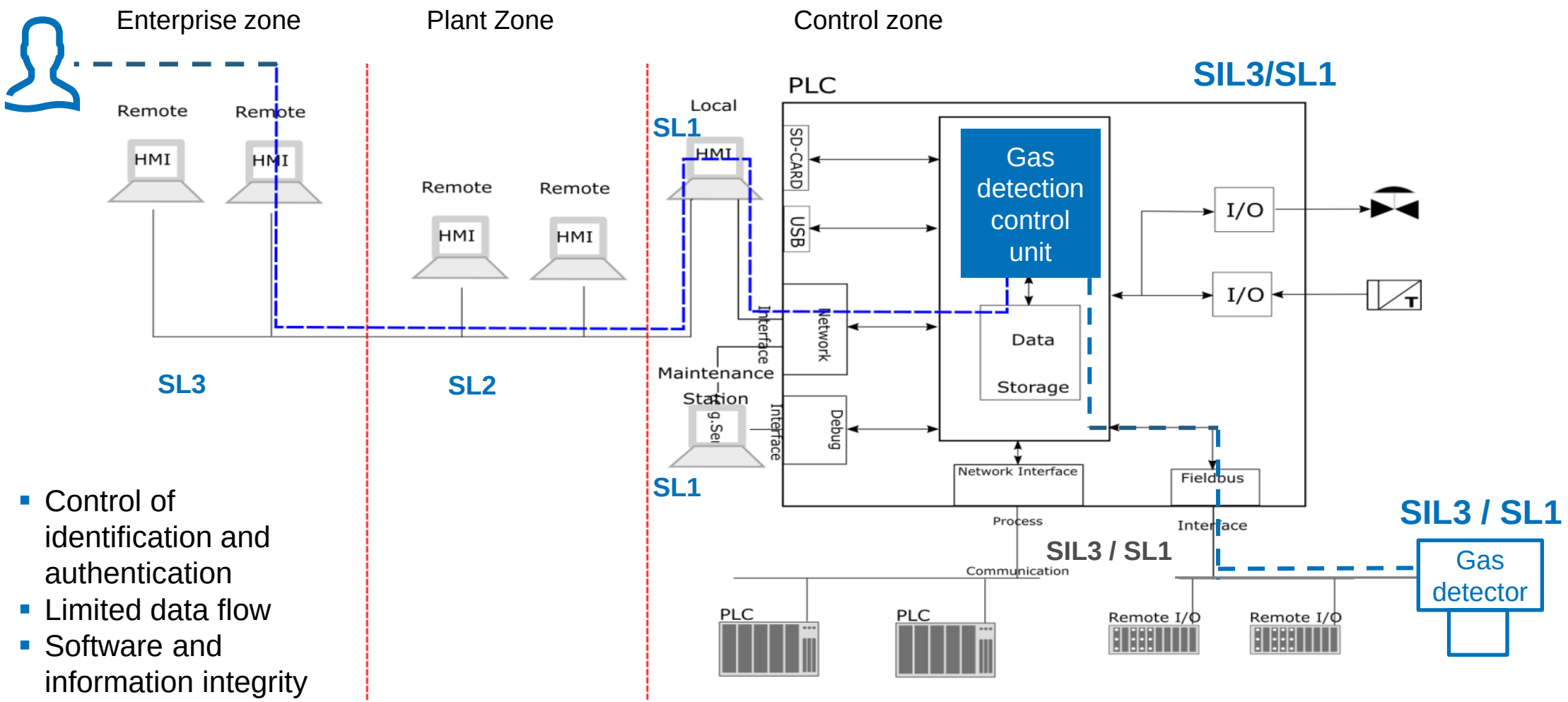
7.5.2.2

„Wenn Bedrohungen …. Identifiziert worden sind, sollte eine Schwachstellenanalyse durchgeführt werden, um die **Security Anforderungen** festzulegen.

ANMERKUNG Siehe **Normenreihe IEC 62443.**

TÜVRheinland®
Genau. Richtig.

Welches SL für welche Zone?



- Control of identification and authentication
- Limited data flow
- Software and information integrity
- Use control

TÜVRheinland®
Genau. Richtig.

Vielen Dank!

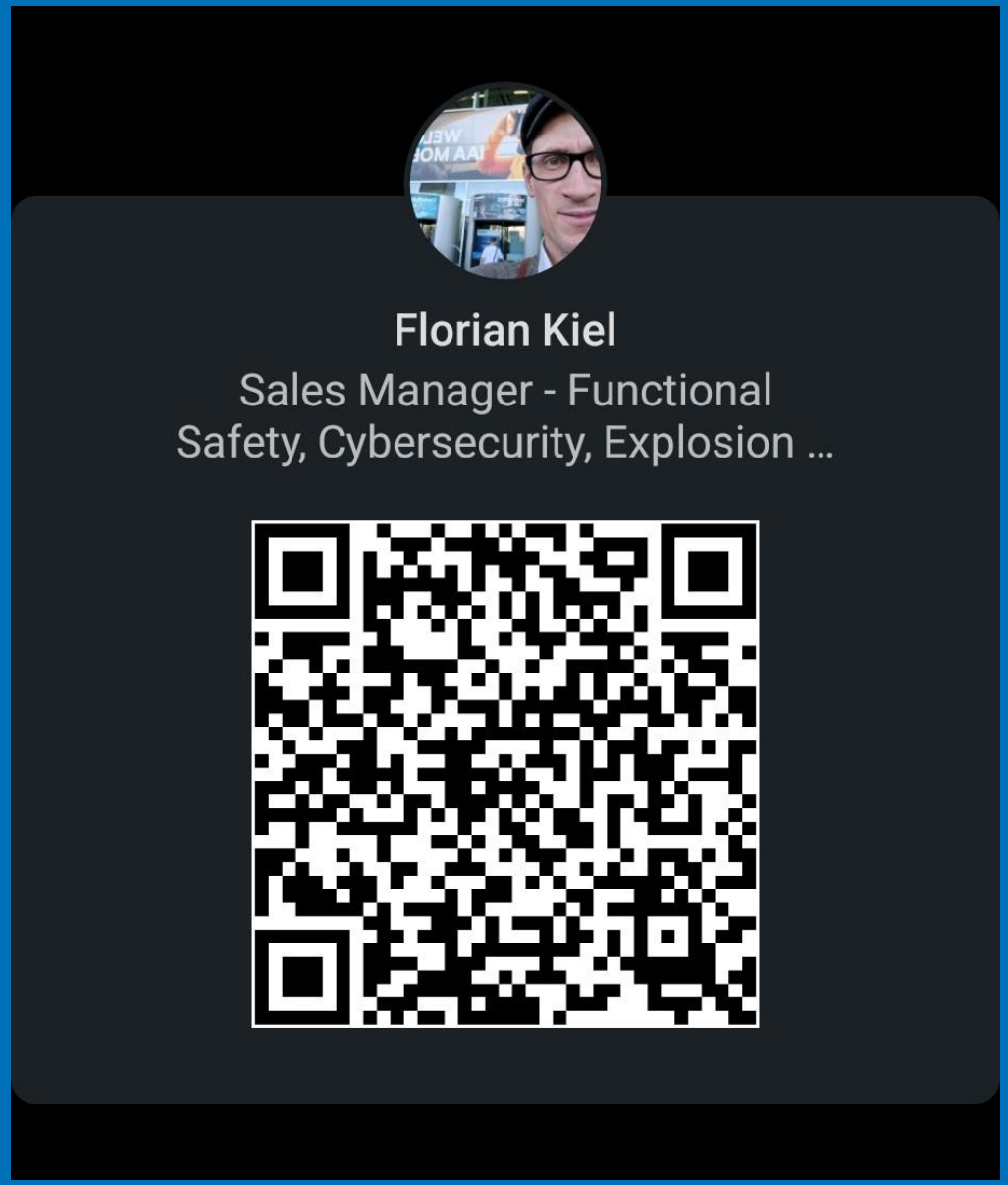
Florian Kiel

Field Sales Executive

Functional Safety & Cybersecurity & Explosion Protection
E-Mail: florian.kiel@tuv.com
Tel.: +49 221 806 4355
Mob.: +49 1722 13 23 83

Erfahren Sie mehr auf unserer Webseite

https://www.tuv.com/world/en/ot-security.jsp



TÜVRheinland®
Precisely Right.