Cybersecurity auf dem Prüfstand:

Das Zusammenspiel von Regulierung und Standard für Unternehmen und Produkte

Florian Kiel
Functional Safety & Cybersecurity

TÜVRheinland®
Precisely Right.

Sachlage

Ist ein Budget für Cybersecurity notwendig?

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

Entwicklungen

Was tut sich im Digitalen Kontext?

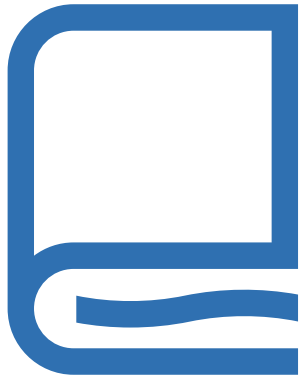
- Zunehmende Vernetzung von Anlagen & Systemen
- Umgebungen mit unterschiedlichen Schutzzielen
- Fachkräftemangel und Akzeptanz von Managed Services
- Steigende Zahl und Qualität von Cyberangriffen
- stetiger Anstieg regulatorischer Anforderungen

TÜVRheinland®
Precisely Right.

Regulierungen

Welche Anforderungen müssen erfüllt werden?

- KRITIS, IT-Sicherheitsgesetz 2.0, BetrSichVO
- EU NIS-2 Regulierung – Network Information Security
- EU CRA – Cyber Resilience Act ab 11.12.27
- EU RED – Radio Equipment Directive ab 01.08.25
- EU MVO – Maschinenverordnung ab 20.01.27
- UN ECE R155 – Automotive Cybersecurity
- andere *branchenspezifische Regulierungen…*

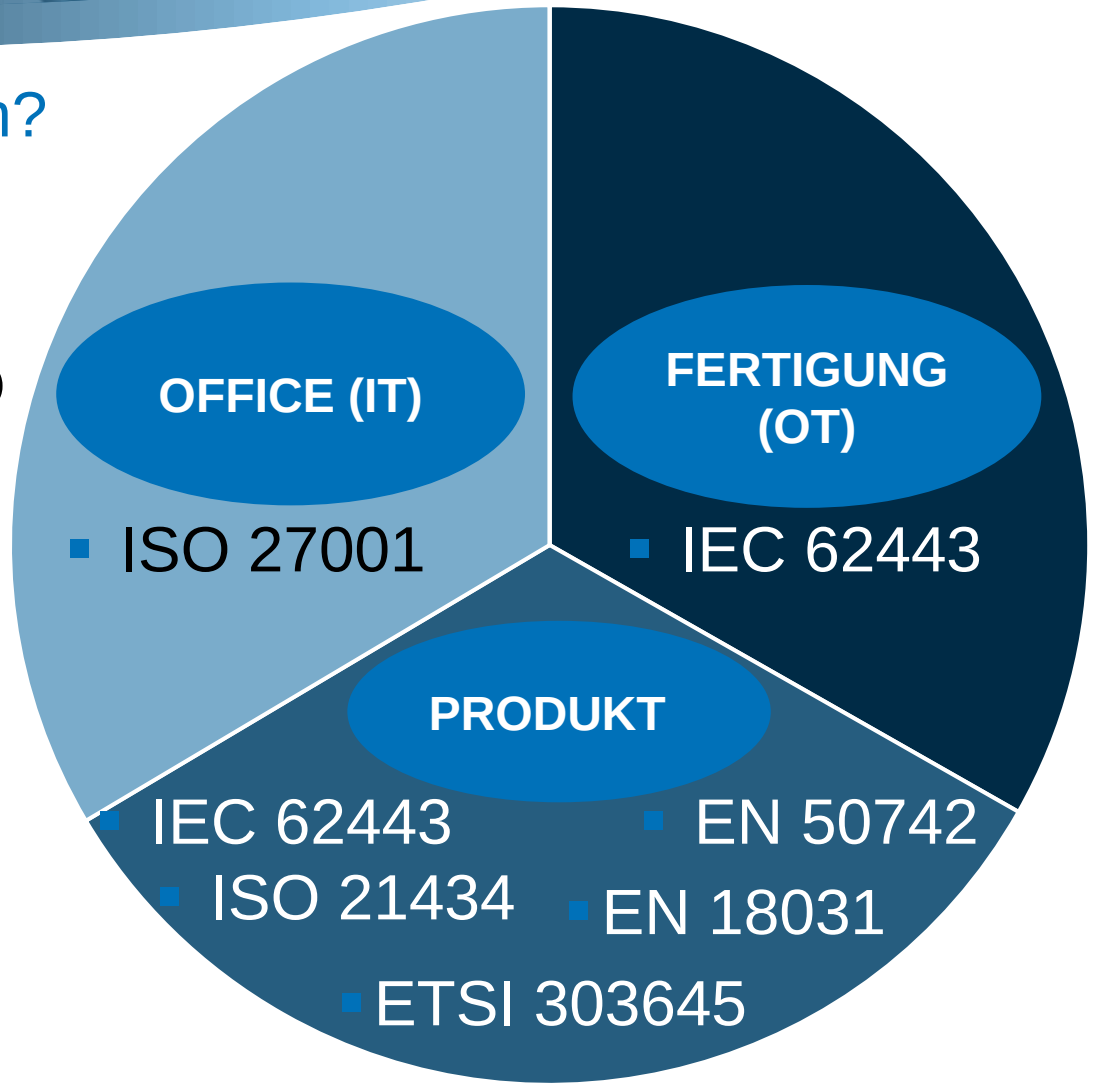


TÜVRheinland®
Precisely Right.

Unternehmen

Was ist zu betrachten?

- NIS-2 / DSGVO



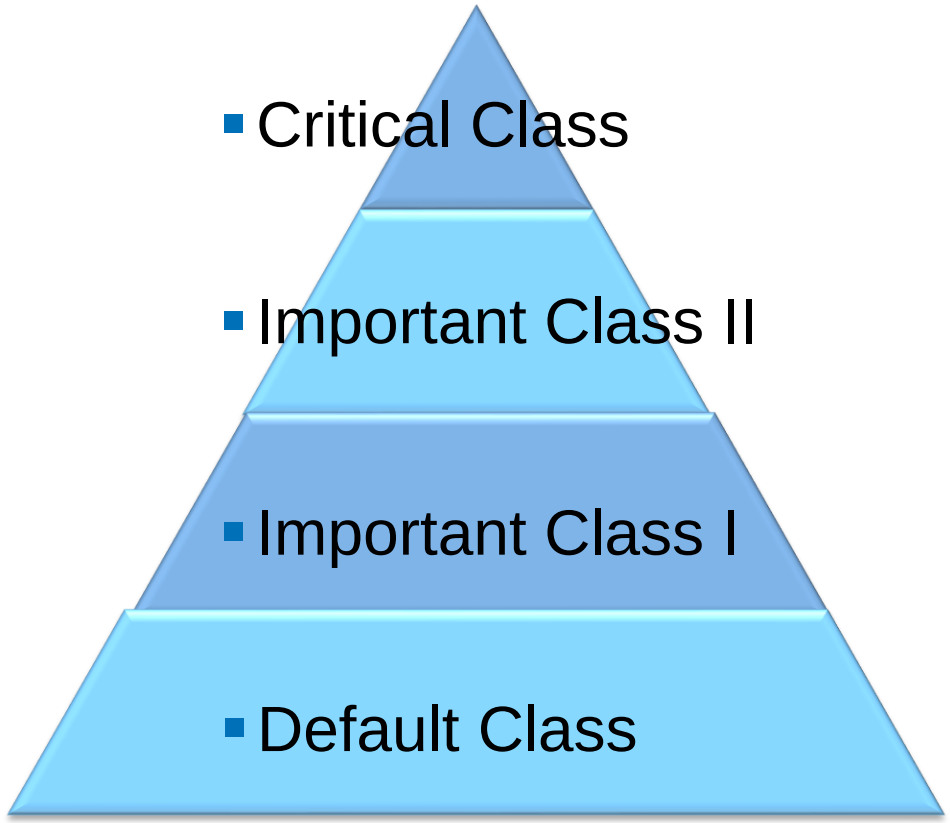
- BetrSichVO
- CRA / MVO / RED / R155

TÜVRheinland®
Precisely Right.

Produkte

EU CRA - Cyber Resilience Act

- Produkte mit digitalen Elementen: Hardware oder Software
- Alle Produkte auf dem EU-Markt / sofern nicht anders reguliert
- Herstellererklärung mittels CE-Zeichen; Bewertung in Einzelfällen über unabhängige Dritte
- Meldepflichten, kostenlose Updates, hohe Geldbußen



- *Ausnahmen: nicht kommerz. OpenSource* Software, Medical, Automotive, Machinery, Aviation…*

TÜVRheinland®
Precisely Right.

Cybersecurity nach IEC 62443

Generell	IEC-62443-1-1 Terminologie, Konzepte und Modelle	IEC-62443-1-2 Terminologie, Konzepte und Modelle	IEC-62443-1-3 Metriken für die Einhaltung der Systemsicherheit	
Regeln und Prozeduren	IEC-62443-2-1 Anforderungen an das IACS-Sicherheits-Managementsystem	IEC-62443-2-2 Implementierungs-anleitung für ein IACS-Sicherheits-Managementsystem	IEC-62443-2-3 Patch-Management im IACS-Umfeld	IEC-62443-2-4 Anforderungen an IACS-Lösungsanbieter
System	IEC-62443-3-1 Sicherheits-Technologien für IACS	IEC-62443-3-2 Sicherheits-Risikobewertung und System Design	IEC-62443-3-3 Systemsicherheits-Anforderungen und Sicherheitsebenen	
Komponenten	IEC-62443-4-1 Anforderungen an Produktentwicklung	IEC-62443-4-2 Technische Sicherheits-Anforderungen für IACS-Produkte		

Betreiber

Service Provider

Hersteller

TÜVRheinland®
Precisely Right.

IEC 62443 Standard

EU CRA – Cyber Resilience Act
EU RED – Radio Equipment Directive
EU MVO / MR Machinery Regulation

- CRA – harmonisierter Standard: ??? - in Arbeit oder IEC 62443???
- RED – harmonisierter Standard: EN 18031 verfügbar
- MVO – harmonisierter Standard: EN 50742 in Arbeit

- Viele Unternehmen nutzen die Normenreihe IEC 62443
- IEC 62443 deckt in Teilen die Anforderungen der RED
- IEC 62443 ist Stand der Technik, weil häufig referenziert und weiträumig anwendbar

TÜVRheinland®
Precisely Right.

EU Cyber Resilience Act (CRA)

- Aktuell sind keine Harmonisierten Standards vorhanden

- Hauptthemen:
  - ANNEX I: Part I - Essential Cybersecurity requirements
  - ANNEX I: Part II - Vulnerability Handling Requirements
  - ANNEX II: Information and Instructions to the user
  - ANNEX VII: Contents of the technical documentation

- TÜV Rheinland ”Mapping” der CRA Anforderungen in Bezug auf IEC 62443

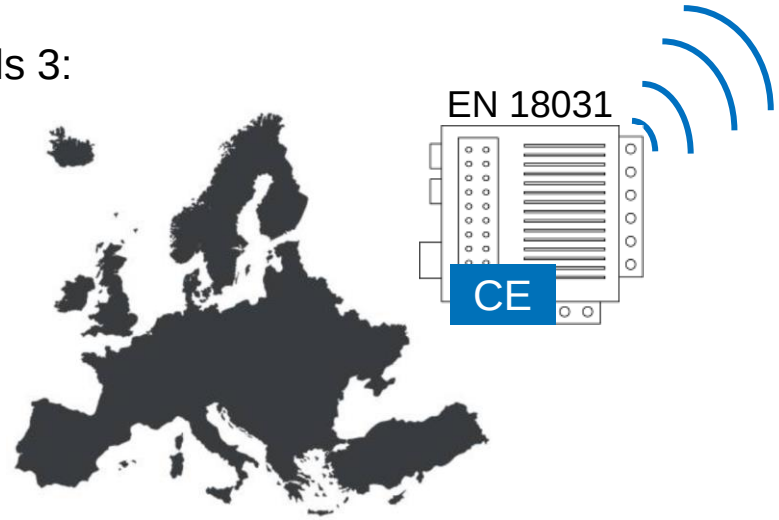
- Gap-Analyse basierend auf IEC 62443 mittels TÜV Rheinland Procedure Checklist (PCL) zum Nachweis der Konformität mit dem EU CRA

! Wer jetzt bereits startet, riskiert kleine inhaltliche Lücken, die geschlossen werden müssen, um harmonisierte Standards zu erfüllen. Der TÜV Rheinland sieht die IEC 62443 als eine solide Basis zum Nachweis der CRA Konformität.

TÜVRheinland®
Precisely Right.

EU Radio Equipment Directive (RED)

- Hersteller ist verantwortlich für Identifikation anwendbarer Teile des RED Artikels 3:
  - (d) - EN 18031-1
  - (e) - EN 18031-2
  - (f) - EN 18031-3



- Durchführung eines Assessments basierend auf der EN 18031

- TÜV Check Liste stellt die Anforderungen des Assessments

- Der “Decision Tree” muss für jede Anforderung ausgefüllt werden
  - falls notwendig: Nachweise für “Functional Completeness Assessment” (Entwicklungsdokumentation) und “Functional Sufficiency Assessment” (Testergebnisse) vorlegen
- Zusätzlich: Threat Model, Security Tests und Nutzerhandbücher vorlegen

! Die finale Entscheidung der Zertifizierung obliegt der offiziell Benannten Stelle (TÜV Rheinland Products GmbH).

TÜVRheinland®
Precisely Right.

Safe the Date!

EU Cyber Resilience Act & EU Radio Equipment Directive

WANN: 03. oder 04.06.2025

WO: TÜV Rheinland LGA Products GmbH
Am Grauen Stein, 51105 Köln

Anmeldung unter: Cyber Security Days 2025

Das erwartet Sie:

- Fundierte Informationen zu den neuesten regulatorischen Vorgaben und Cybersicherheitsanforderungen der EU, einschließlich CRA und RED
- Praxisnahe Einblicke zur Umsetzung von Cybersicherheitsmaßnahmen über den gesamten Lebenszyklus hinweg, von der Produktentwicklung bis zu regelmäßigen Updates während der Nutzung
- Safety vs. Security – Diskussion einprägsamer Beispiele aus der Praxis und mit Live-Demo eines Penetrationstests
- Strategien zur Absicherung von Produkten und Produktionsprozessen gemäß den IEC 62443-Standards
- Klärung individueller Fragen im direkten Austausch mit unseren Expertinnen und Experten

TÜVRheinland®
Precisely Right.

Vielen Dank für die Aufmerksamkeit.

Florian Kiel
Field Sales Executive
Functional Safety & Cybersecurity
E-Mail: florian.kiel@tuv.com
Tel.: +49 221 806 4355
Mob.: +49 1722 13 23 83

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

TÜVRheinland®
Precisely Right.