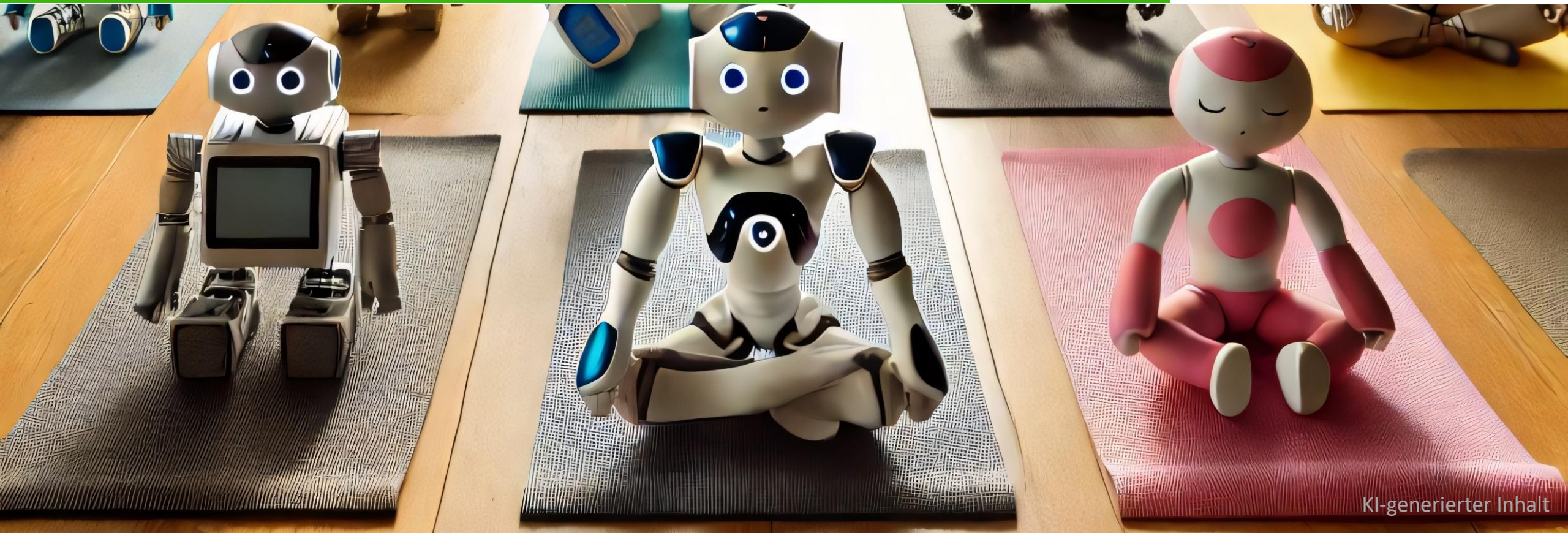
CYBER RESILIENZ ACT IN DER AUTOMATISIERUNG

Was gilt jetzt und was kommt noch?

Christopher Polt, 13. Januar 2026

MURR ELEKTRONIK

stay connected



KI-generierter Inhalt

Das ist MURRELEKTRONIK

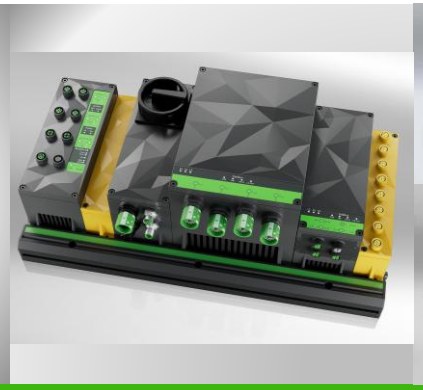
- Firmensitz in Oppenweiler
- Gegründet im Jahr 1975 von Franz Hafner
- Unternehmen in Familienbesitz
- Über 3.200 Mitarbeiter weltweit
- In mehr als 50 Ländern vertreten
- 5 Produktionsstandorte
- Über 1 Mio. Artikel auf Lager

MURRELEKTRONIK ist Ihr starker Partner

Murrelektronik

Portfolio

SCHALTSCHRANK-ELEKTRONIK



STEUERUNGSTECHNIK

NETZWERKTECHNIK

IO-LINK DEVICES

INTELLIGENTE STROMVERTEILUNGSSYSTEME

SCHNITTSTELLEN

IO-SYSTEME

ANSCHLUSSTECHNIK

In allen BRANCHEN zu Hause

Lager- & Fördertechnik

Food & Beverage & Packaging

Gebäudetechnik

Automotive

Werkzeugmaschinen

Flughafen-Logistik

Mobile Anwendungen

IN UNTERSCHIEDLICHSTEN BRANCHEN ZU HAUSE
Profitieren Sie von unserer branchenübergreifenden Erfahrung

About me

Gesetze sind Spielregeln: Und wer den CRA nicht einhält, der darf dann in Zukunft einfach nicht mehr mitspielen.

Christopher Polt, Global Application Engineer Network Technologies – Murrelektronik GmbH
#iscybercertified

Christopher Polt
Global Application Engineer Network Technologies
Christopher.polt@murrelektronik.de
+49 176 810 4392
Murrelektronik GmbH
Grabenstraße 29, Oppenweiler

Warmup

Grundlagen CRA (Welche Produkte sind betroffen? / Wer muss wie handeln?)

Quick glance:

- Betroffen sind alle Produkte mit digitalen Elementen (PwDE). Handeln müssen Hersteller und Distributoren beim Inverkehrbringen auf den europäischen Binnenmarkt.
- Eine Inverkehrbringung von Produkten ohne CRA-Konformität ist nach Anwendungsbeginn untersagt.

Was hat die EU vor?

Cyber Resilience Act

Zielsetzung

- Schutz von Verbrauchern und Unternehmen durch:
  - Erhöhung des Security-Niveaus von in Verkehr gebrachten *Produkten (Hard- und Software) mit digitalen Elementen*
  - Garantierten Investitionsschutz von erworbenen *Produkten (Hard- und Software) mit digitalen Elementen* durch längeren Support-Zeitraum.

- Verbesserung der Cybersicherheitsstandards durch:
  - Formulierung von verbindlichen Cybersicherheitsanforderungen an Hersteller und Integratoren.
  - Erhöhung der Innovationsbereitschaft der herstellenden Unternehmen

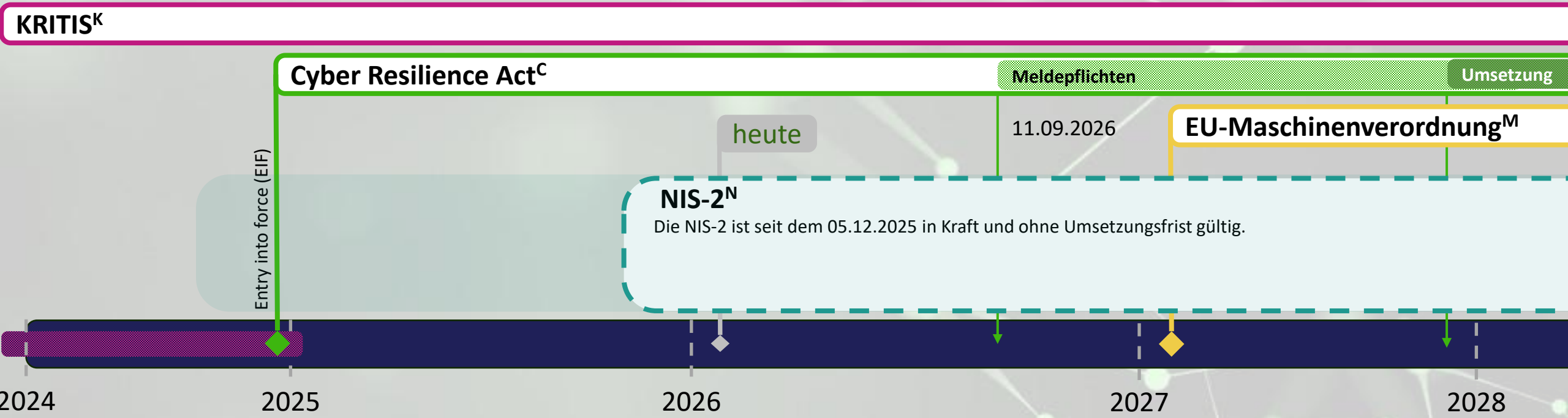
- **Erleichterung der Produktauswahl durch:**
  - **Reglementierung des Marktzugangs von nicht konformen Produkten**
  - **Ausweitung der CE-Kennzeichnung auf den Bereich Cyber-Sicherheit**

Wer schummelt, darf nicht mehr mitspielen …

Produkte mit digitalen Elementen [nach CRA]: Ungefähr: Alle Produkte mit externer oder interner Netzwerkschnittstelle

Zeitstrahl

EU-Gesetze



[C] Cyber Resilience Act, ab 11.12.2027. Regelt neue Anforderungen an Produkte im Bereich Cybersicherheit für europäischen Marktzugang.

[K] KRITIS: physische Sicherheit und Resilienz, KRITIS-Betreiber betroffen, Umsetzung bis 10/24 bei EU danach bei Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

[M] Neue Maschinenverordnung der EU ab Januar 2027. Keine Safety mehr ohne Security. Es gibt bereits einen Draft der harmonisierten Norm prEN 50742.

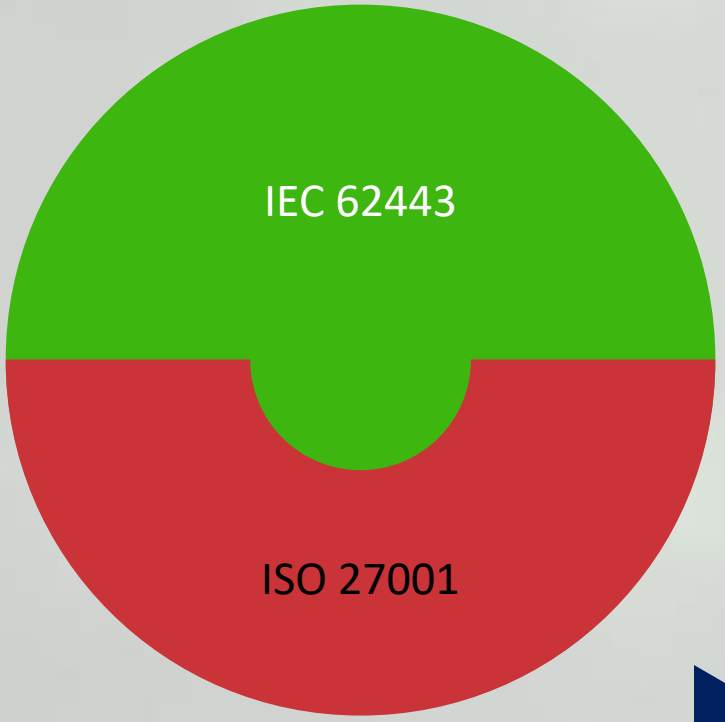
[N] NIS-2 betroffen sind KRITIS-Betreiber & wichtige und sehr wichtige Einrichtungen. Schutzobjekt sind über 30.000 Unternehmen in Deutschland. Die Richtlinie wurde in ein Bundesgesetz überführt und ist seit dem 05.12.2025 gültig.

Cyber Resilience Act

Eine Einordnung

- Ziel der Security-Standards ist die Erhöhung der Cybersicherheit für Unternehmen.
- Die EU gießt diese Forderungen von Unternehmen erstmalig in allgemeingültige Gesetze.
- Risikobasierter Ansatz

Anerkannte Security-Standards



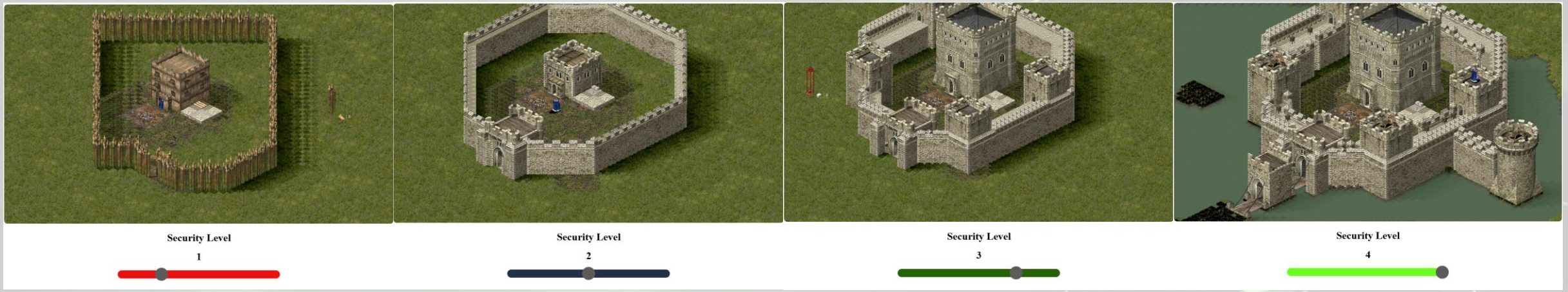
EU Cyber-Security Richtlinien/Verordnungen

Erhöhtes EU-Sicherheitsniveau

IEC 62443-4-2

Security Levels

- 62443-4-1 – Vergleichbar mit der Zertifizierung, dass ich Burgen bauen darf.
- 62443-4-2 - Vergleichbar mit einer Blaupause wie eine „quantifizierbar sichere“ Burg gebaut werden muss.
- Freiwilligkeit: Umsetzung liegt nur beim Unternehmen.

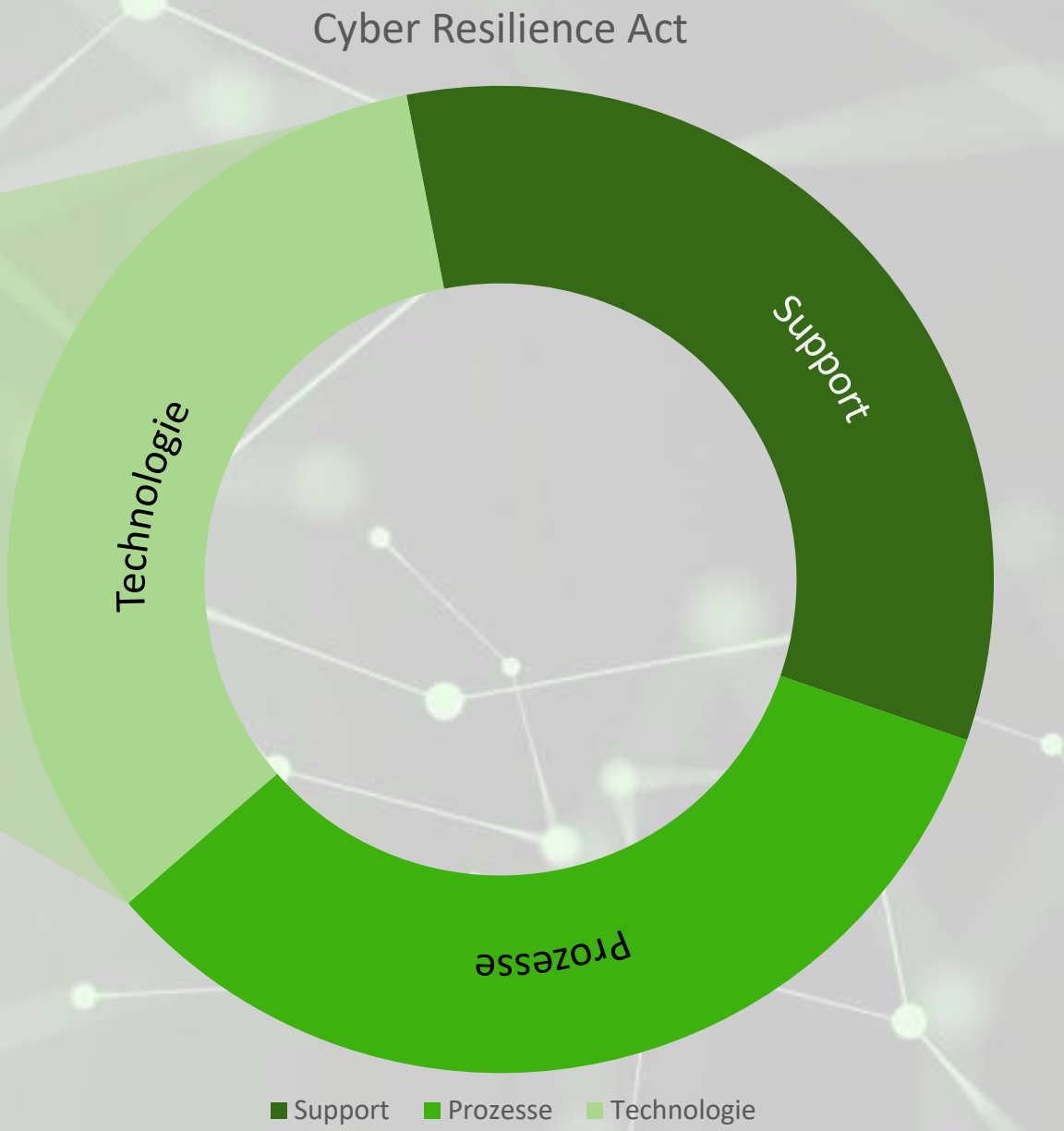


Schutz vor versehentlicher Fehlbedienung	Schutz vor Angriffen

Cyber Resilience Act

IEC 62443 Relevante Teile

- **62443-1-5**: Scheme for IEC 62443 security profiles
- **62443-3-3**: System security requirements and security levels
- **62443-4-1**: Secure product development lifecycle requirements
- **62443-4-2**: Technical Security requirements for IACS components
- **62443-6-2**: Security evaluation methodology for IEC 62443



Cyber Resilience Act

Risikobasierter Ansatz

Risiko = Bedrohung x Schwachstelle x Auswirkung

Risiko = Wahrscheinlichkeit x Auswirkung

Risikoanalyse

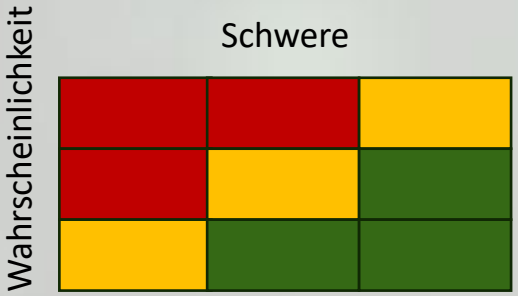
- Gefährdung innerhalb des Netzwerks
- Möglichkeit, dass kritische Prozesse betroffen sind
- Folgen eines Angriffs auf das Asset

Unterhalb des tolerierbaren Levels

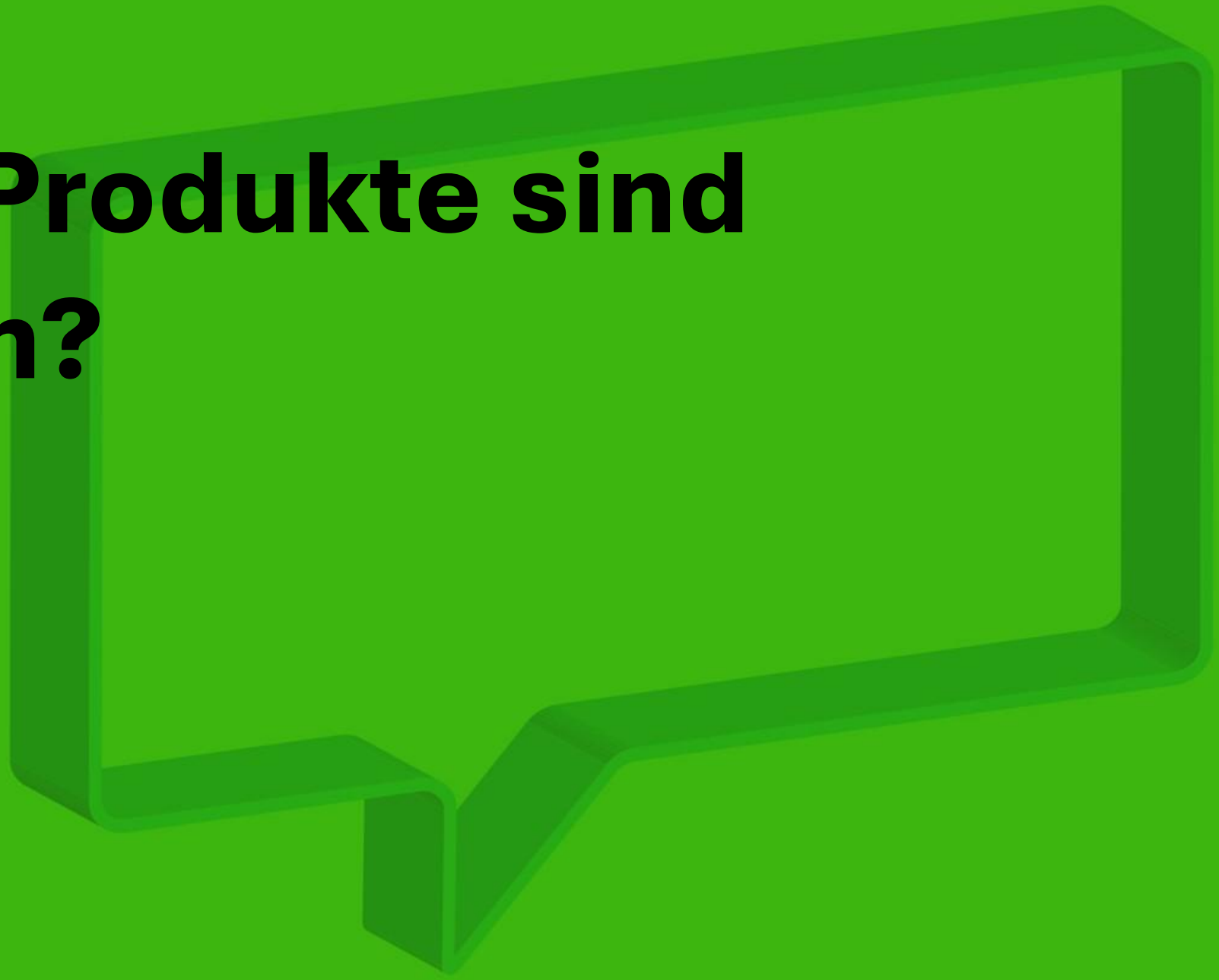
ja → Keine weiteren Schritte nötig

nein → Weitere Schritte nötig wie:

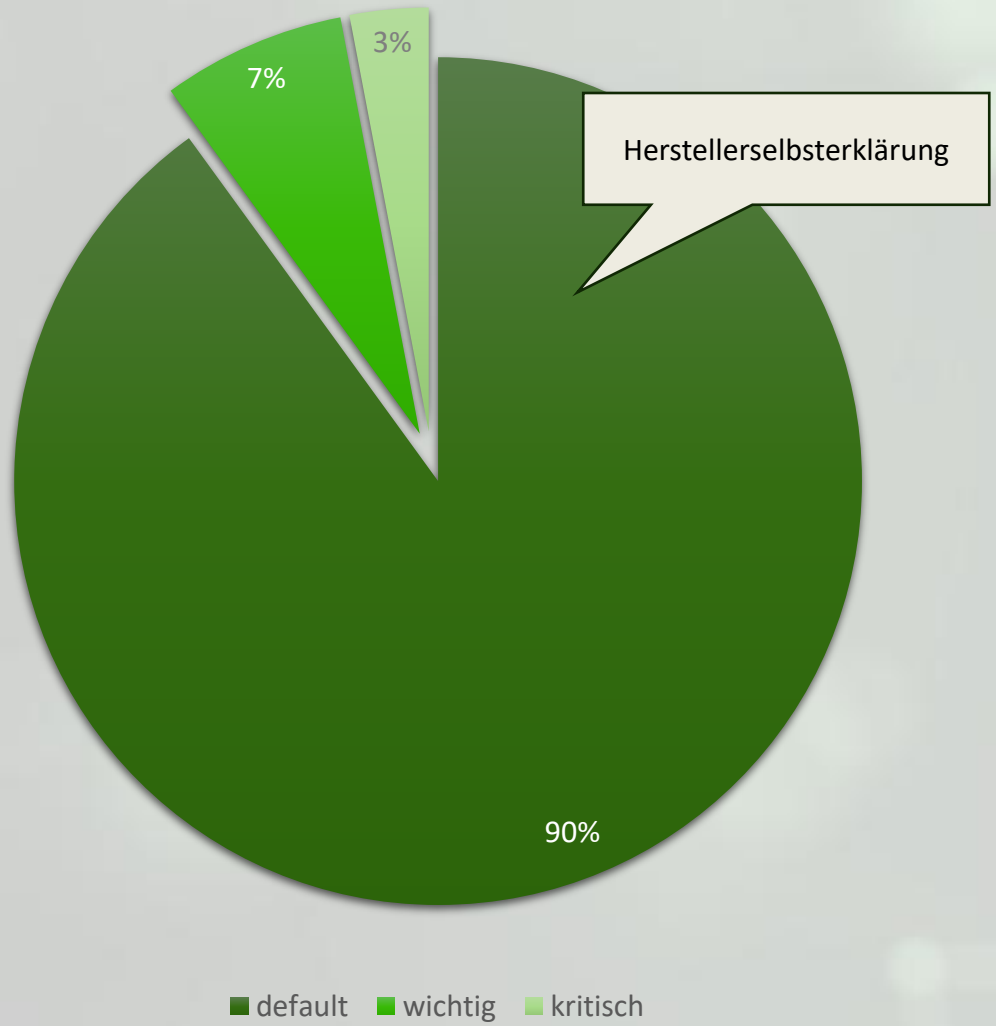
- Isolation
- Netzwerksegmentierung
- Virtualisierung
- Patching
- Verschlüsselung



Welche Produkte sind betroffen?



„Produkte mit digitalen Elementen“



Mechanische oder elektronische Sperrung einer Schnittstelle hebelt den CRA nicht aus!

Default-Kategorie

Nicht im Anwendungsbereich:

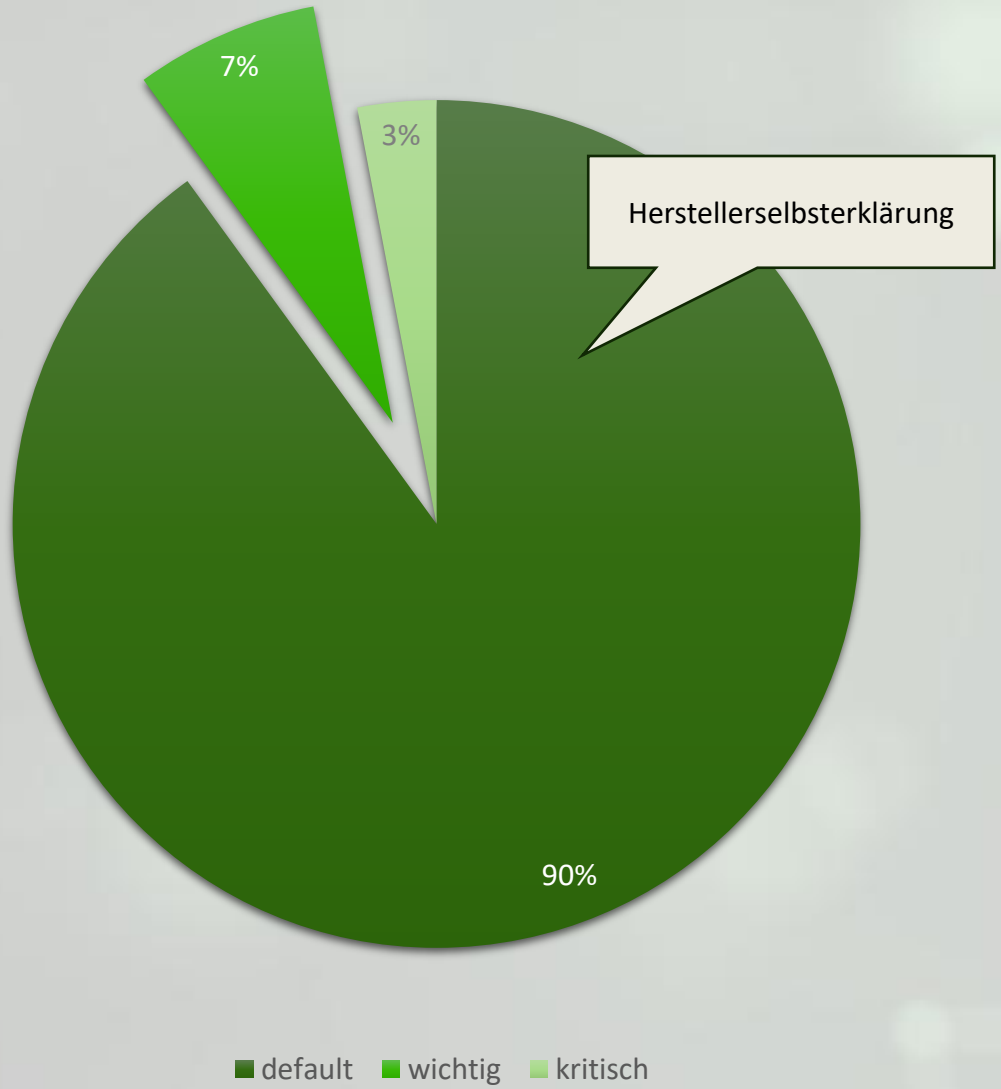
- Medizinprodukte
- In-vitro-Diagnostika
- Kraftfahrzeuge
- Zivilluftfahrt
- Schiffsausrüstung
- Produkte, die ausschließlich für militärische Zwecke konzipiert sind.
- Ersatzteile, die identische Bauteile ersetzen und, die nach denselben Spezifikationen hergestellt werden wie die Bauteile, die sie ersetzen
- Produkte, die vor der Anwendung des CRA in Verkehr gebracht werden.
- Software-as-a-service (SaaS)

Im Anwendungsbereich:

- Produkte mit digitalen Elementen (Maschinen, Anlagen und Software, Komponenten mit interner oder externer Netzwerkschnittstelle)
- Bestandsprodukte[I] nach wesentlichen Veränderungen nach dem Stichtag.
- Land- und forstwirtschaftliche Maschinen

[I] Produkte, deren Inverkehrbringung bereits vor dem Stichtag erfolgte.

„Produkte mit digitalen Elementen“



Wichtige Produkte mit digitalen Elementen

Klasse 1:

- Identitätsmanagementsysteme
- Browser und Password-Manager
- Antiviren-Software
- VPN und Netzwerkmanagementsysteme, Router und Modems und Switche
- SIEM-Systeme
- PKI und Zertifikatsausstellung
- Physische und virtuelle Netzwerkschnittstellen
- Betriebssysteme
- Mikroprozessoren, Mikrocontroller, FPGA und ASIC mit sicherheitsrelevanten Funktionen
- Assistenten für Heimautomation
- Produkte mit Sicherheitsfunktionen für die häusliche Überwachung
- Babyüberwachungssysteme und internetfähiges Spielzeug (sprechen, filmen, orten)
- Wearables

Klasse 2:

- Hypervisoren und Containerlaufzeiten
- Firewalls, IDS und IPS
- Manipulationssichere Mikroprozessoren und -controller

Cyber Resilience Act

Betroffene Produktfamilien

PG4	Modlight (IO-Link)
	Modlight60 Pro RGB (IO-Link)
	IO-Link Control Devices
PG5	MVK Pro / Impact Pro
	MVK / Impact67
	Cube67
	Cube20/Cube20S
	IO-Link Hubs
	IO-Link Converters
	Xelity
PG6	IO-Link Control Devices
PG9	Emparro IP67 Hybrid
	Emparro20-Pro IO-L Adapter

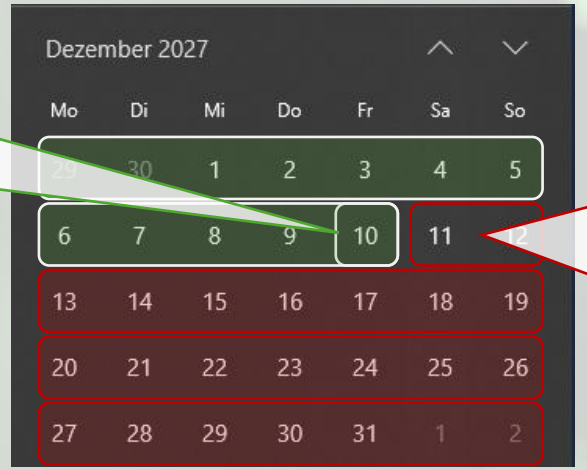
Vario X

Cyber Resilience Act

Anwendungsbereich

„Nur der Zeitpunkt der Inverkehrbringung zählt“

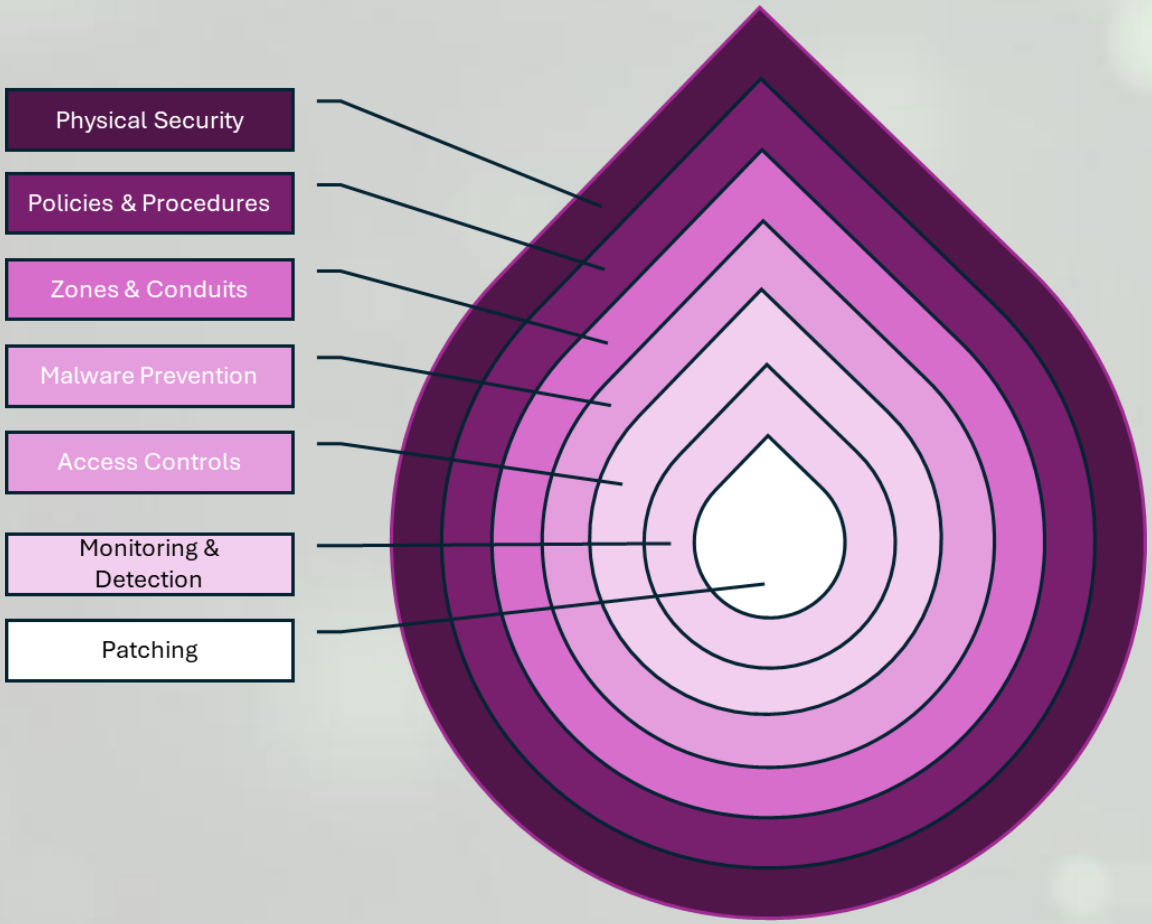
Ein vor dem 11.12.2027 in Verkehr gebrachtes Produkt unterliegt nicht dem CRA



während das identische Produkt der gleichen Serie, das nach dem 11.12.2027 in Verkehr gebracht wurde, dem CRA unterliegt.

Cyber Resilience Act

Herstellerpflichten (Art. 13)



Defense-in-Depth nach IEC 62443-4-2

Dokumentationspflichten:
- Risikoanalyse
- SBOM (Software Bill of Material): Auflistung aller verwendeten Dritthersteller-Softwarebibliotheken (CycloneDX oder SPDX)

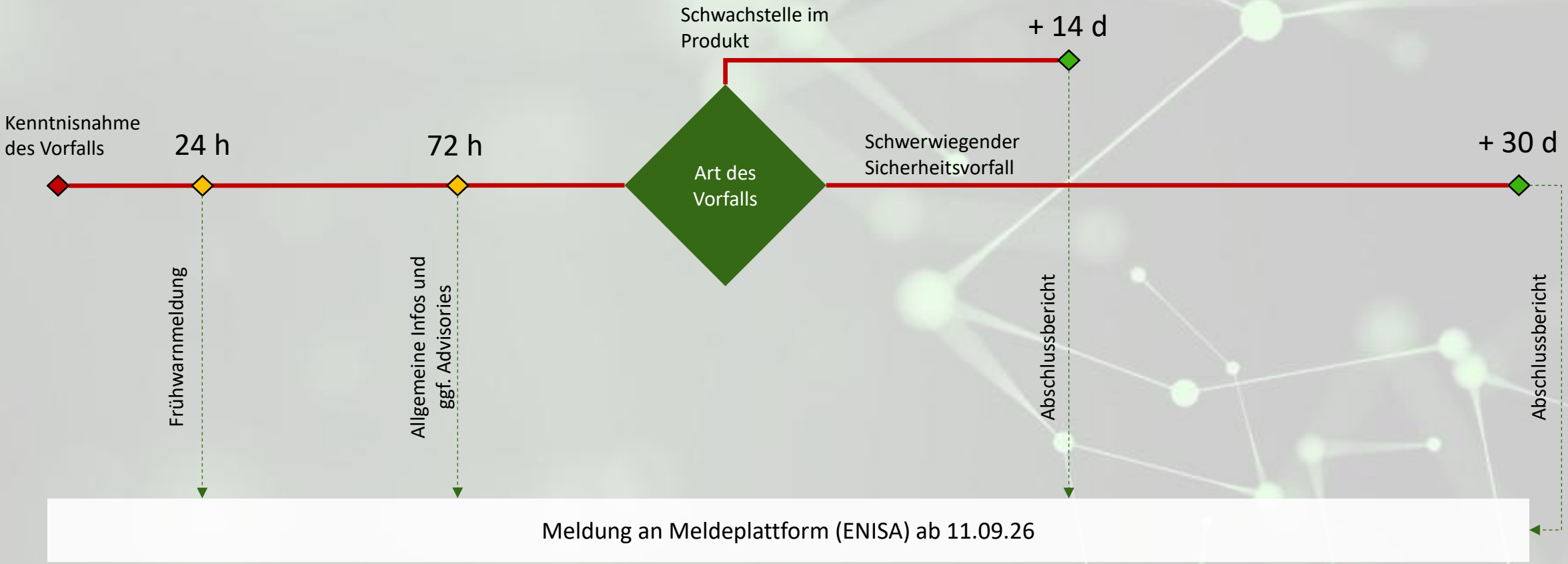
Supportpflichten und -garantien:
- Kostenlose Bereitstellung von Security-Updates für:
  - mindestens 5 Jahre oder
  - über die Lebensdauer des Produkts
- Einrichtung eines PSIRT (Product Security Incidence Response Teams)

Freiheit von Schwachstellen beim Inverkehrbringen
- Aktives Monitoring von Schwachstellen
- Meldepflichten (Art.14)

Anwendung des cybersicheren Produktlebenszyklus (nach 62443-4-1)
- Security-by-Default
- Defense-in-Depth

Cyber Resilience Act

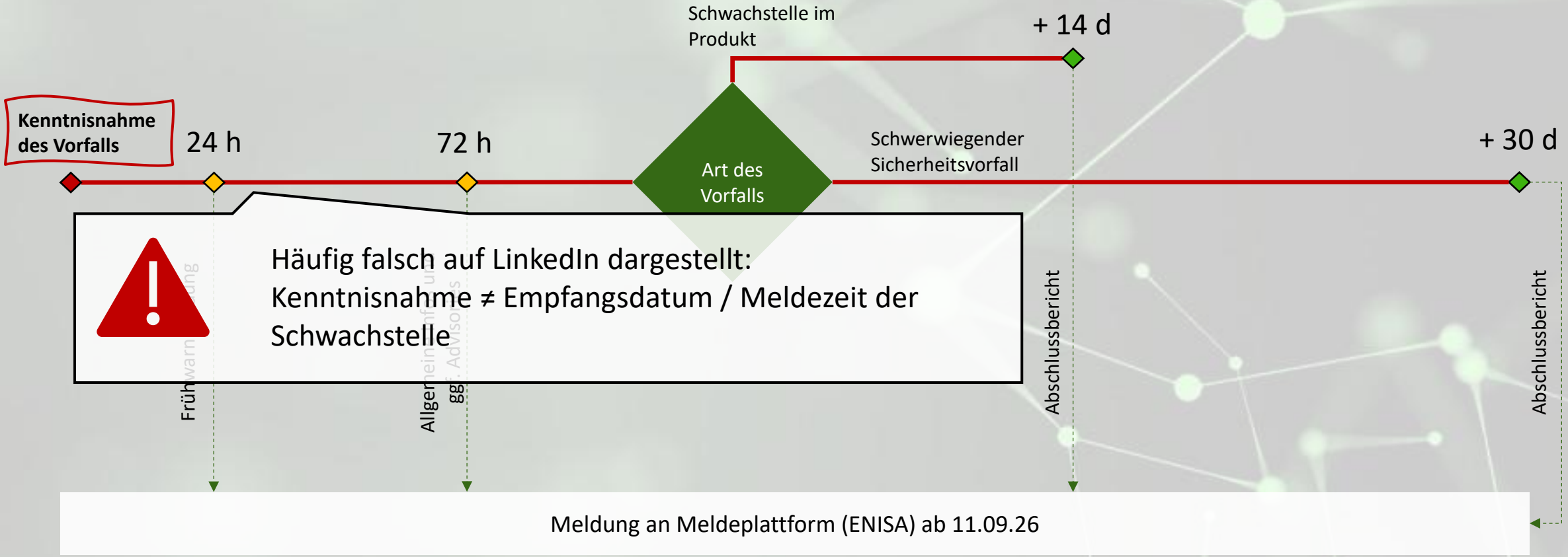
Meldepflichten (Art. 14)



- Aktuell bedeutet das, dass alle PwDEs (auch die, die vor dem 11.09.2026 in Verkehr gebracht wurden [keine Bestandsregelung] unter diese Meldepflichten fallen.

Cyber Resilience Act

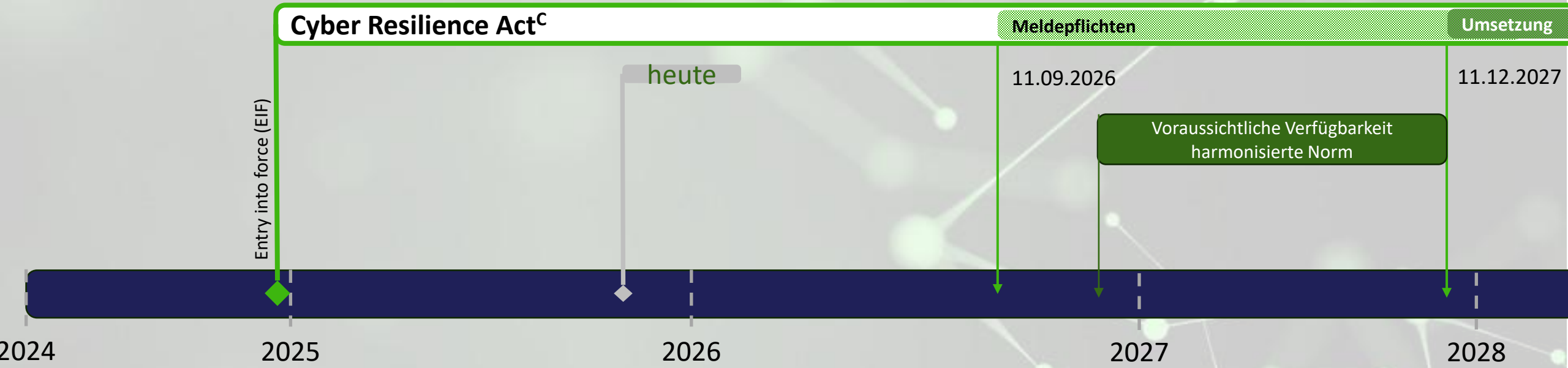
Meldepflichten (Art. 14)



Aktuell bedeutet das, dass alle PwDEs (auch die, die vor dem 11.09.2026 in Verkehr gebracht wurden [keine Bestandsregelung] unter diese Meldepflichten fallen.

Cyber Resilience Act

ME Timeline



CRA Readiness

- Hard-, Firm- und Software sind für den CRA vorbereitet.
- Finalisierung ist aufgrund von fehlenden Normen noch nicht möglich.
- CRA-Conformance aus CRA-Ready-Produkten wird durch Firm- und/oder Software-Update hergestellt.

CRA Conformance

- CE-Konformität hergestellt.
- Produkt kann nach Anwendungsbeginn (11.12.2027) noch verkauft werden.

Welche Aktivitäten gibt es innerhalb der ME rund um den CRA?

- Interne und externe Trainings und Vorträge
- Mitwirkung bei den wichtigen Verbänden
  - VDMA
  - ZVEI
  - Feldbusnutzerorganisationen
  - VDECert: Advisories und CSAF
- Interne **CRA-Taskforce**
- Formierung eines Product Security Incidence Response Teams (**PSIRT**) seit 2023
  - Portfolioanalyse
  - GAP-Analyse
  - ME-interne Security Spezifikation

CRA

Zusammenfassung

- ✓ Sich auf die Neuerung einlassen.
- ✓ Unterschiede und Gemeinsamkeiten zwischen CRA und den relevanten Normenteilen der IEC 62443 erkennen und verstehen.
- ✓ Sich der Verpflichtungen und der Timeline bewusst werden.
- ✓ Risikoanalyse für in Frage kommende Produkte durchführen.
- ✓ Notwendige Prozesse einführen
- ✓ Einbindung der eigenen Lieferkette in den Security-Prozess und in den Dialog mit Lieferanten vor dem 11.12.2027 gehen.
- ✓ Unterstützung bei Lieferanten und Dienstleistern suchen.

- ✓ Nicht den Kopf in den Sand stecken.


Vielen
Dank!
MURR
ELEKTRONIK
stay connected

Questions?