Willkommen

Cyber Resilience Act

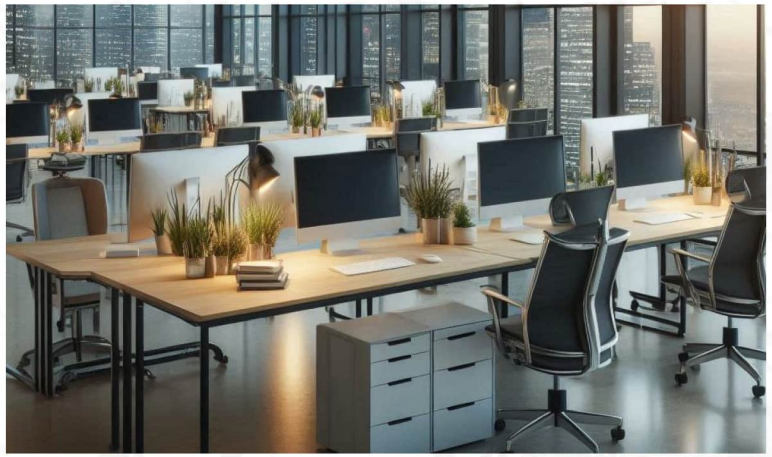
Grundlegende Anforderungen der neuen EU-Verordnung

Agenda

- Einstieg/Motivation
- Cyber Resilience Act
  - Einordnung
  - Anforderungen
  - Produktklassifizierung

Grundlagen

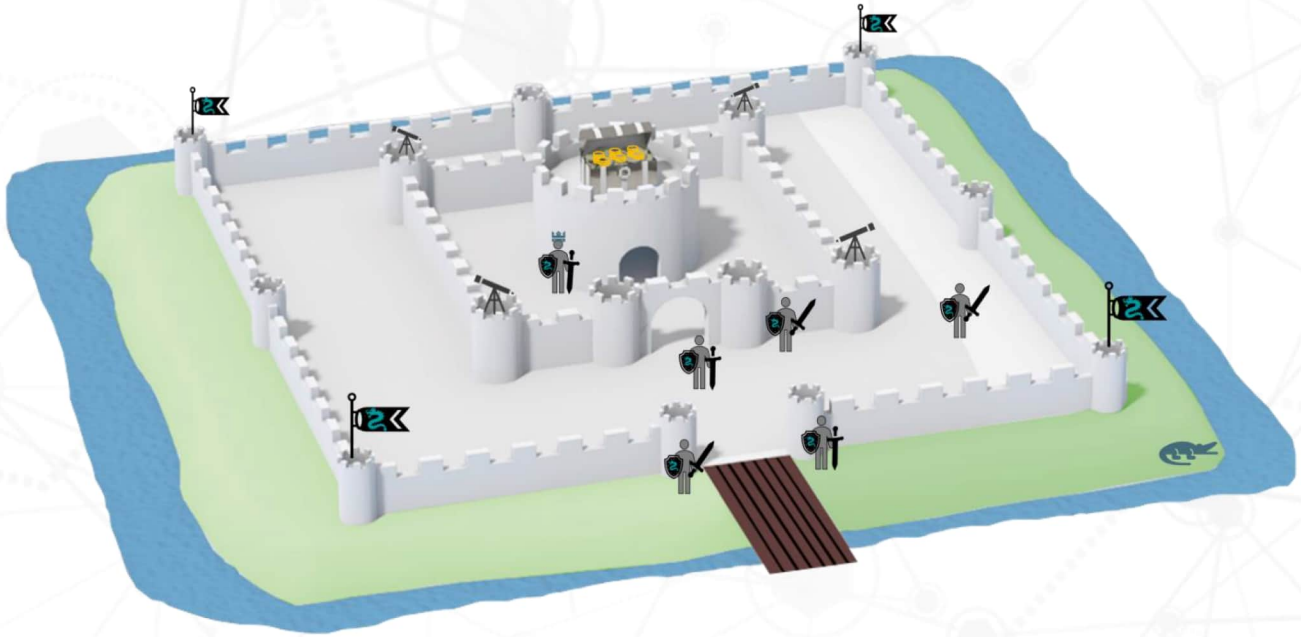
Einstieg



Quelle: AI

Quelle: AI

Das „Defense in Depth“ Konzept

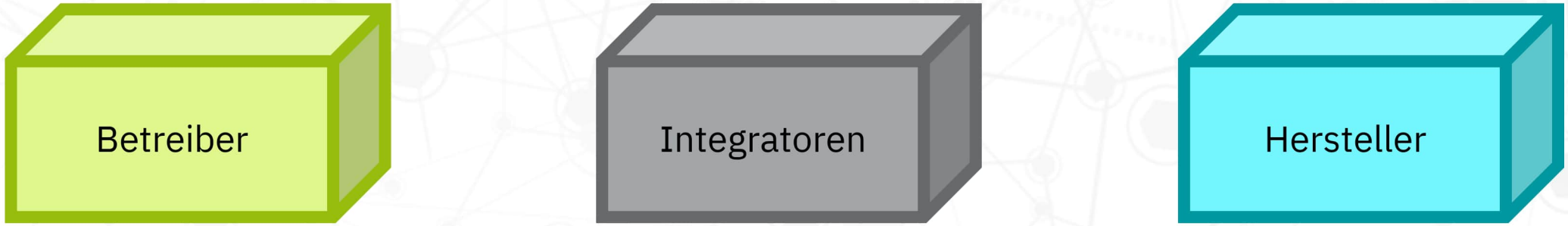


Mehrere Verteidigungslinien

- Wassergraben
- Mauern
- Wachtürme
- Bewaffnete Ritter
- Zugbrücke

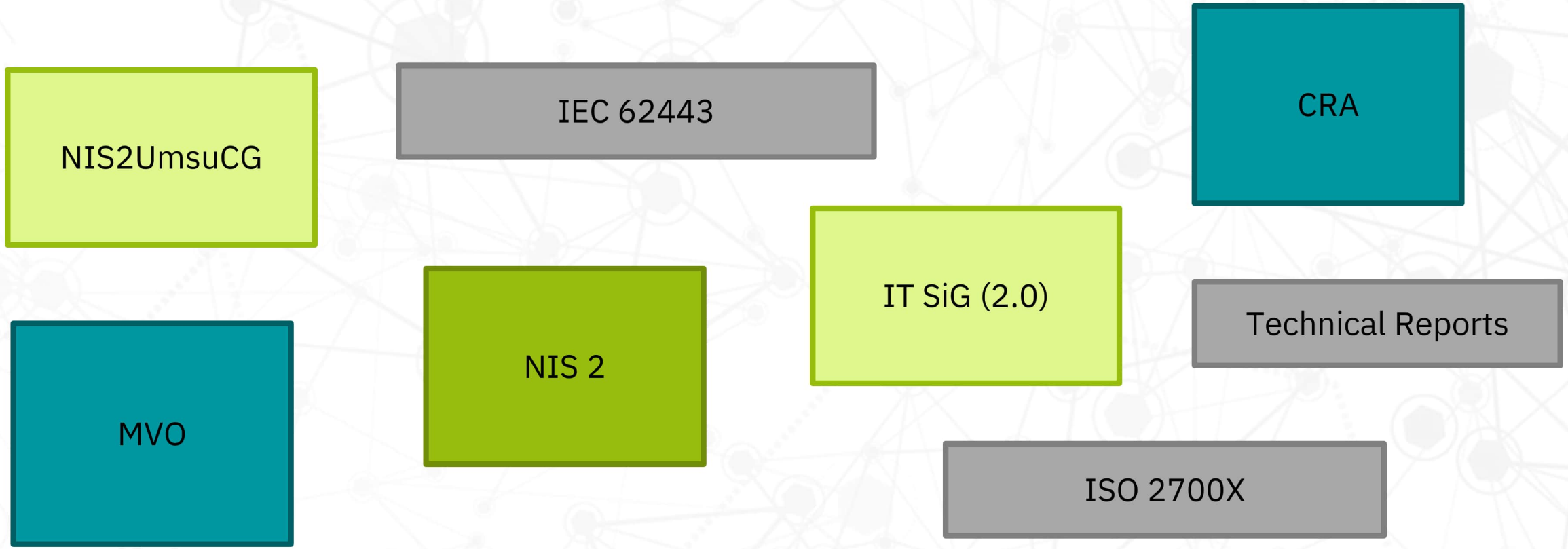
Kontext

EU-Agenda:
Stärkung der **Cybersicherheit**



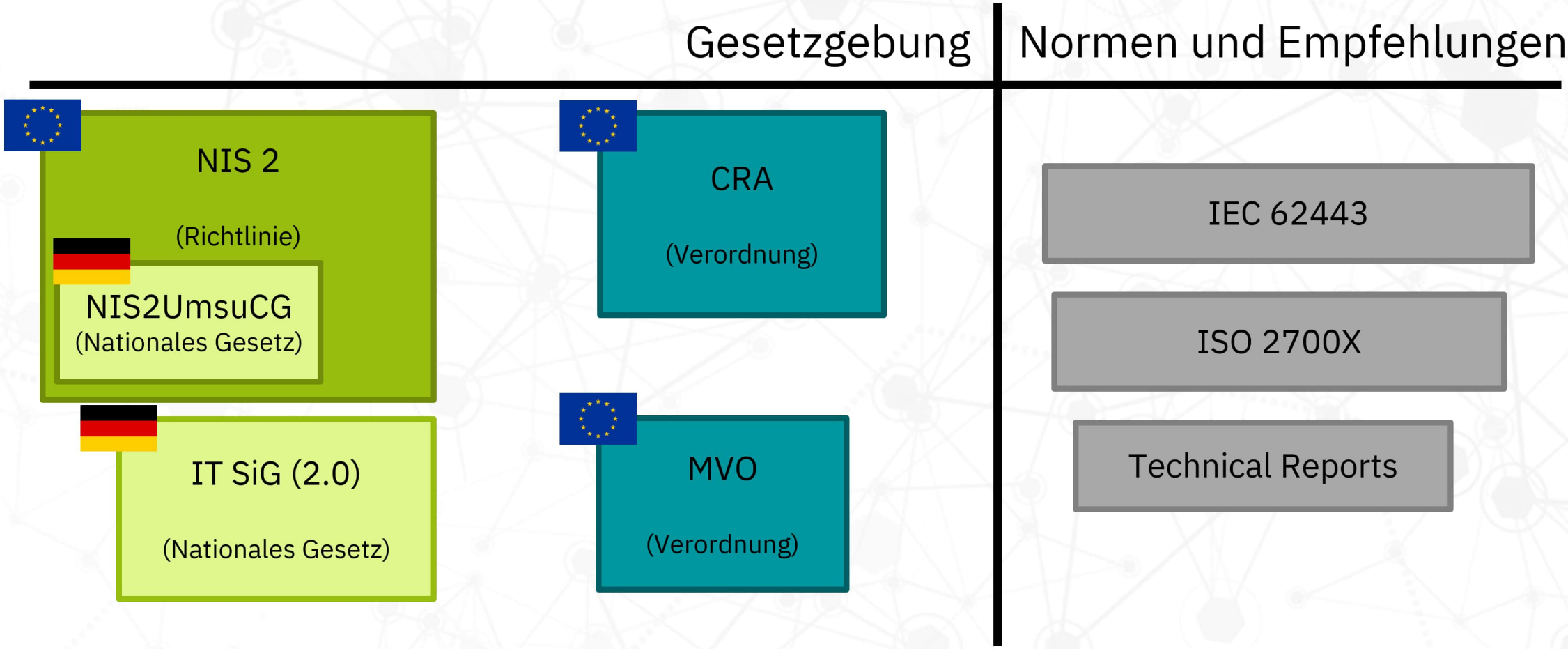
Cyber Resilience Act

Abgrenzung



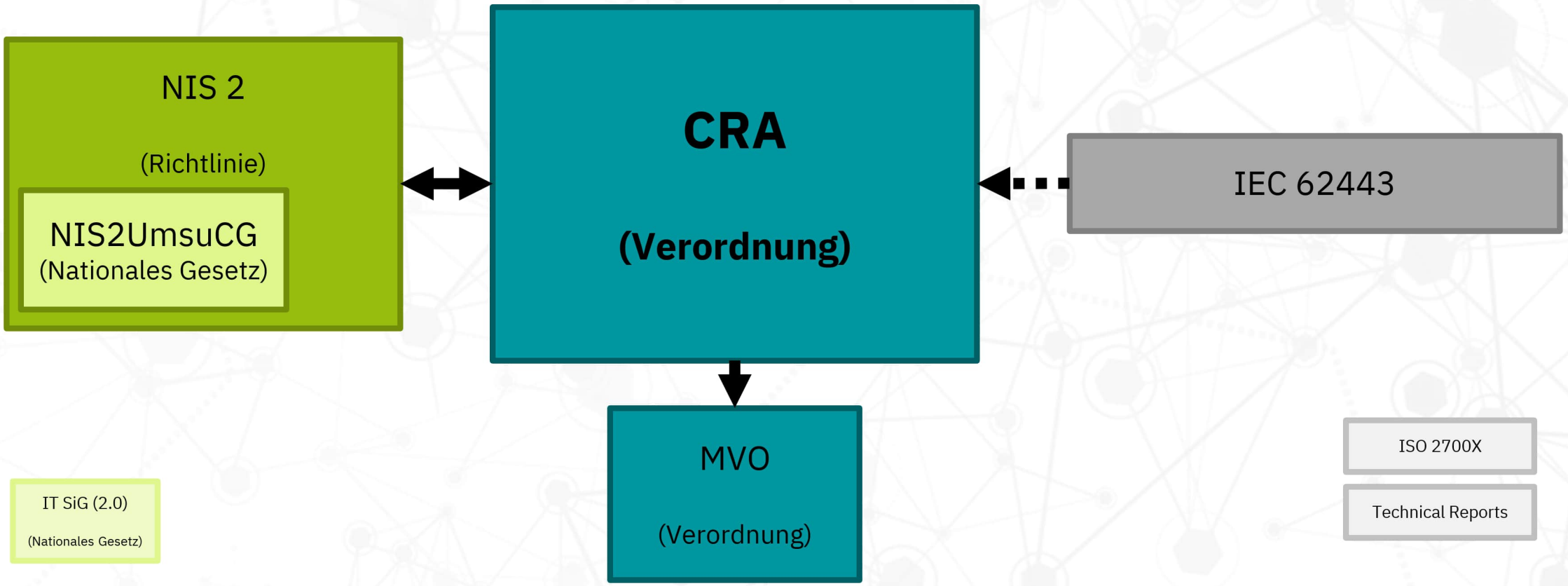
Cyber Resilience Act

Abgrenzung



Cyber Resilience Act

Wechselwirkungen



Cyber Resilience Act

CRA: Hintergrund und Motivation

- Verbesserung des Binnenmarktes
- Verbesserter Grad der Cybersicherheit in der EU
- Rolle der EU im Bereich Cybersicherheit
- Sicheres Internet ist relevant für kritische Infrastrukturen

CRA: Anforderungen und Pflichten

- Adressiert Hersteller und Inverkehrbringer von Produkten mit **digitalen** Elementen
- Es muss erklärt werden, dass das Produkt über einen definierten Zeitraum **cybersicher** betrieben werden kann
  - Über den Lebenszyklus
- Schwachstellen müssen entdeckt, gemeldet und behoben werden -> **Prozess**
- Konformität fließt in die **CE-Erklärung** mit ein
  - Eigenerklärung oder extern auditiert, je nach Kategorie
- **Geldbuße** bis zu 15.000.000€ oder 2,5% weltweiter Umsatz

CRA: Anforderungen und Pflichten

- Pflichten für Hersteller, (Markt-)Einführer und Händler
  - Hersteller haben die umfangreichsten Auflagen
    - Z.B. besondere Meldepflichten
  - Händler und andere dritte können bei Veränderungen zum Hersteller werden
  - Dokumentationen müssen erstellt und 10 Jahre vorgehalten werden
  - Pflichten hängen zusammen:
    - Z.B. Händler muss Pflichten von Hersteller und Einführer prüfen, bevor er vertreibt

Cyber Resilience Act

CRA: Technische Anforderungen

- Sichere Standardkonfiguration
- Schutz von Verfügbarkeit, Integrität und Vertraulichkeit
- Überwachung (z.B. Logging)
- Sicheres Zugriffskonzept und sichere Datenübertragung
- Möglichkeit alle Daten zurückzusetzen und/oder zu löschen

Cyber Resilience Act

CRA: Schwachstellenbehandlung

Dokumentation von Komponenten & Schwachstellen

- Erfordert SBOM

Regelmäßige (Sicherheits-)Tests

Unverzügliche Patches für **Schwachstellen**

- Wenn möglich automatisiert
- Informationen zu gepatchten Schwachstellen
- Sicherheitspatches kostenlos (*)

Möglichkeiten für Meldungen + Disclosure-Strategie

Cyber Resilience Act

CRA: Informationen für den Nutzer

Anforderungen, welche Informationen einem Produkt beiliegen

- Kontaktinformationen, Adresse + Digital
- Meldekontakt für Schwachstellen
- Eindeutige Produktidentifikation
- Anwendungsbereich, Funktionalität und Sicherheitsumgebung

Cyber Resilience Act

CRA: Informationen für den Nutzer

Anforderungen, welche Informationen einem Produkt beiliegen

- Vorhersehbare Umstände, die zu Cyberbedrohungen führen können
- Informationen zu Support(-Zeitraum)
- Bedienungsanleitung
- Ggf. SBOM

CRA: Produktklassifizierung

90 % aller Produkte	10 % aller Produkte		
„Normal” Art. 32 (1)	„Wichtig” Klasse I Art. 32 (2)	„Wichtig” Klasse II Art. 32 (3)	„Kritisch” Art. 32 (4) (Art. 8 (1))
“Selbsteinschätzung”	Bewertungsverfahren	Bewertungsverfahren oder Zertifizierung	EU-Zertifizierung
Komponenten:	**Komponenten:**	**Komponenten:**	**Komponenten:**
• Babyphone • Normale Automatisierungs-komponenten • PCs • etc...	• Router • VPN • Teilw. Smart Home Geräte • Passwortmanager • Betriebssysteme • Teilw. Browser • Netzwerkmanagement • SIEM	• Firewalls & IDS/IPS • Manipulationssichere Mikroprozessoren & Mikrocontroller • Hypervisoren & Container	• Hardware-Geräte mit Sicherheitsboxen • Smartcards oder ähnliche Geräte • Smart Meters

Öffentlich (IV)

Mathis Mohr
Industrial Security Consultant

PHOENIX CONTACT
Deutschland GmbH

Tel.: +49 5281 946-2155
E-Mail: mathis.mohr@phoenixcontact.de

Danke

Cyber Resilience Act

Grundlegende Anforderungen der neuen EU-Verordnung