AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

CYBER RESILIENCE ACT: STATUS UND ÜBERBLICK

Christoph Schmittner
Senior Research Engineer
AIT – Digital Safety & Security

EUROPEAN CYBERSECURITY FRAMEWORK

Cyber Security Act

Network and information systems (NIS) directive

Cyber Resilience Act

General Data Protection Regulation (GDPR)

EU cybersecurity strategy

EUROPEAN CYBERSECURITY FRAMEWORK

Cyber Security Act

Network and information systems (NIS) directive

Cyber Resilience Act

General Data Protection Regulation (GDPR)

EU cybersecurity strategy

MOTIVATION

- **Wachsende Cyberbedrohungen**
  - Zunahme von Cyberangriffen mit erheblichen Auswirkungen auf Wirtschaft, Meinungsbildung und Verbrauchersicherheit

- **Geringes Sicherheitslevel**
  - Software, Hardware und IoT-Geräte derzeit nur unzureichend geschützt
  - Mangel an adäquaten Sicherheitsupdates

CYBER RESILIENCE ACT

Der Cyber Resilience Act wird als EU-Vorschrift verpflichtend für die **CE-Kennzeichnung** für **Produkte mit digitalen Komponenten**

Veröffentlichung Herbst 2024 erwartet

Anforderungen müssen ab 2027 erfüllt werden

Nachweis der Konformität nach **Produktklassifizierung**

Intern / Extern / EU Certification Scheme

KERNASPEKTE DES CYBER RESILIENCE ACT

Anforderungen an Cybersicherheit, kontinuierliches Risikomanagement und **regelmäßige Updates** sowie Kommunikation der Sicherheitsmerkmale

Nichteinhaltung als Hersteller: Geldbußen von bis zu 15 Millionen Euro oder 2,5 Prozent des weltweiten Umsatzes

Wissentliches Verstoßen als Betreiber: Strafrechtliche Verantwortung bei Einsatz von Produkten ohne CE-Kennzeichnung

Entzug der Betriebserlaubnis: Wenn CRA-Anforderungen nicht erfüllt werden

WAS SIND PRODUKTE MIT DIGITALEN ELEMENTEN

Produkte mit digitalen Elementen sind

- **Hardware**, **Software** oder **Kombinationen**
  - **indirekt** oder **direkt verbunden** mit anderen Systemen
  - fähig zur **Verarbeitung**, **Speicherung** oder **Übertragung** digitaler **Daten**
  - einschließlich **aller Remote Services** die für eine **Funktion relevant** sind

Verfügbar auf dem europäischen **Markt** mit dem Ziel, **Geld** zu verdienen

SEKTOREN

CRA ist horizontale und für Produkte in **allen Sektoren** verpflichtend

Einige Sektoren sind **ausgeschlossen**

- Produkte mit digitalen Elementen (PDEs) für **nationale Sicherheit** oder **Verteidigung**
- In-vitro-Diagnostika, andere medizinische Geräte, Fahrzeuge, Flugsysteme mit **bereits bestehenden Regelungen mit gleichwertigen Anforderungen**

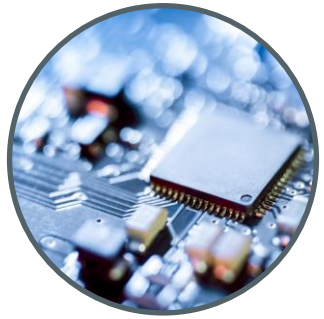
KLASSIFIZIERUNG

Default category

- **Self assessment**
- Smart Speaker, Festplatte, Textverarbeitung

Class I – (important) products

- **Self-assessment (based on harmonized standard) or third party**
- Browser, Virenschutz, Betriebssystem, …



Class II – (highly important) products

- **Third-party assessment (based on harmonized standard)**
- Firewalls, Tamper-resistant Prozessor, …

Kritische Produkte

- **EU cybersecurity certification scheme**
- Smart metering systems, Smartcard, Secure Element

KLASSIFIZIERUNG

Genannte Produkte sind **Beispiele**

EU-Kommission wird Listen ergänzen

Produkte können **umgestuft** werden (5/12 Monate Übergangsfrist)

Faktoren für Klassifizierung

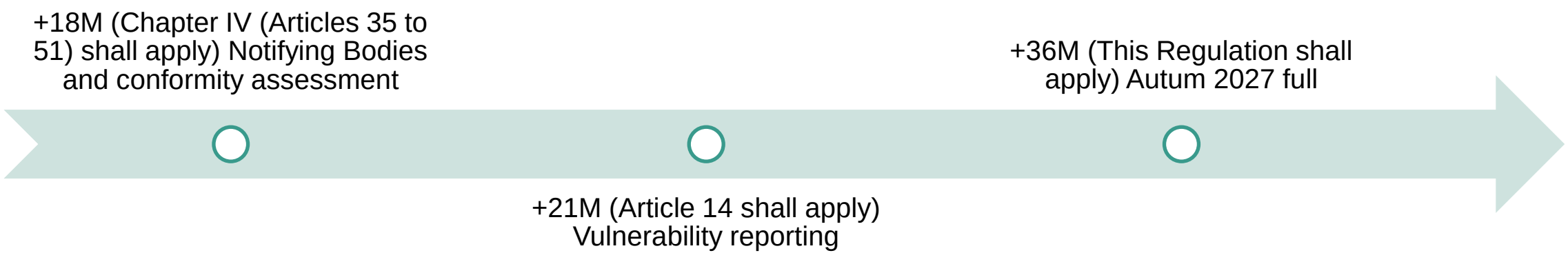
- **Risiko** für andere Produkte oder Nutzer
- Zentrale **Systemfunktionen**
- Verarbeitung **persönlicher Daten**
- Relevant für **Cybersicherheit**
- Einsatz und Relevanz für **wesentliche Dienste**

STROMNETZ

- Kritisches Produkt:
  - **smart metering systems** as defined in Article 2 (23) of Directive (EU) 2019/944
- **Andere Systeme im Smart Meter Bereich sind (noch) nicht erwähnt**
  - Einstufung basierend auf Risiko und Funktionalität, NIS2 Einstufung
- Webservices sind kein Produkt, aber inkludiert, wenn sie eine Funktion eines Produktes ermöglichen

TIMELINE

- **Ankündigung:** **EU’s Cybersecurity Strategy for the Digital Decade** **2020**
- **EC Proposal:** **Cyber Resilience Act** **2022**
- **EP/EC:** **Political agreement on Cyber Resilience Act** **2023**
- **EP Approval:** **MEPs adopt plans** **2024**
- **Consultation of manufacturers:** **June – July** **2024**
- **Publication after EUCO agreement:** **Autum** **2024**
- **20 Days after publication the CRA is in Force:**



AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

CRA FÜR HERSTELLER VON PRODUKTEN MIT DIGITALEN ELEMENTEN

SICHERHEITSORIENTIERTES DESIGN (SECURITY-BY-DESIGN)

AUSTRIAN INSTITUTE OF TECHNOLOGY

- Risikoanalysen während Planung, Design, Entwicklung, Produktion, Lieferung und Wartungsphasen
- Analyse basierend auf Verwendungszweck, Einsatzumgebung, Assets und Nutzungsdauer
- Welche Sicherheitsanforderungen werden umgesetzt und wie wird damit ein akzeptables Risiko erreicht
- Dokumentation der Analyse, resultierender Anforderungen und Umsetzung
- Systeme von Anfang an sicher konfiguriert und Update-fähig

SUPPORT

Erreichte Sicherheit soll über Produktlebenszeit gewährleistet werden

Standard-Support Periode sind 5 Jahre

- außer Lebenszeit oder Nutzungsdauer weicht ab

Verantwortung des Herstellers sicherzustellen dass Schwachstellen erkannt, gemeldet und darauf reagiert wird

- Auch für Open Source oder integrierte Komponenten

Letzte Version im Fokus:

- Hersteller müssen Sicherheitsupdates nur für die neueste Softwareversion anbieten, sofern ältere Versionen kostenlos aktualisiert werden können.
- Für inkompatible Hardware, wie ältere Smartphones, sind Updates für die letzte kompatible Betriebssystemversion vorgesehen

UPDATES FÜR PRODUKTE MIT DIGITALEN ELEMENTEN (PDE)

Neue Zulassung bei Updates die:

- Anwendungsbereich ändern
- Relevante neue Funktionen hinzufügen
- Leistung ändern
- Neue Schnittstellen hinzufügen

Keine neue Zulassung bei

- Security-Updates
- Optische / UI Updates
- Minimale Funktionsupdate

OPEN-SOURCE-SOFTWARE

- Open Source Software **ohne Gewinnabsichten** ist ausgenommen

- Gewinnabsichten liegen vor wenn die **geplanten Einnahmen** die Kosten für **Entwicklung** und **Bereitstellung** übersteigen
  - Beratungs- und Anpassungsleistungen
  - Sammeln von Daten, sofern nicht für Sicherheit, Kompatibilität oder Interoperabilität erforderlich
  - Spenden

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

CRA FÜR BETREIBER VON PRODUKTEN MIT DIGITALEN ELEMENTEN

SYNERGIE ZWISCHEN CRA UND NIS2

01

Regelmäßige Updates: CRA fordert regelmäßige Sicherheitsupdates für digitale Produkte, die die Resilienz und Sicherheit der von NIS2 betroffenen Entitäten verbessern.

02

Höhere Sicherheitsstufen für kritische Produkte: Produkte mit digitalen Elementen, die in wesentlichen Entitäten gemäß NIS2 verwendet werden, müssen nach CRA strengere Sicherheitsanforderungen erfüllen.

03

Lieferkettensicherheit: CRA unterstützt die Einhaltung der NIS2-Lieferkettenanforderungen durch Sicherheitsvorgaben für digitale Produkte.

BESCHAFFUNG - TIMELINE

Derzeit	Keine Auswirkung
Nach CRA-Veröffentlichung	Keine direkten Auswirkungen Berücksichtigung für Nachbeschaffung
12 Monate nach Veröffentlichung	Veröffentlichung der erweiterten Listen mit Einstufungen
36 Monate nach Veröffentlichung	Beschaffung von Produkten mit digitalen Elementen ohne CRA Compliance strafrechtlich relevant Betrachtung von Verwendungszweck und Einstufung • Relevanz ob PDE für wesentliche Dienste eingesetzt wird

BESCHAFFUNG - RAHMENBEDINGUNGEN

- **Mitgliedstaaten** sind für den Schutz der **Infrastruktur verantwortlich**

- EU schafft **Rahmenbedingungen**
  - z.B. 5G Toolbox, ermöglicht Vorgaben auf nationaler Ebene für Beschaffung

Security implications of China-owned critical infrastructure in the European Union

https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702592/EXPO_IDA(2023)702592_EN.pdf

BESCHAFFUNG - RAHMENBEDINGUNGEN

Texts adopted

Wednesday, 17 January 2024 - Strasbourg

Security and defence implications of China's influence on critical infrastructure in the European Union

Resolution europäisches Parlament an EU-Kommission

- ≈ **Diversifizierung von Beschaffung** für Risikominimierung
- ≈ Erweiterung der EU-Verordnung zum **Screening ausländischer Direktinvestitionen (FDI)** auf alle Beteiligungsformen
- ≈ Bewertungen von **Infrastrukturprojekten** mit nicht-EU-Beteiligten, einschließlich einer **Prüfung der Besitzverhältnisse** und **Abhängigkeiten in Lieferketten**
- ≈ **Angleichung von Vorgaben** in Mitgliedsstaaten

https://www.europarl.europa.eu/doceo/document/TA-9-2024-0028_EN.html

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

THANK YOU!

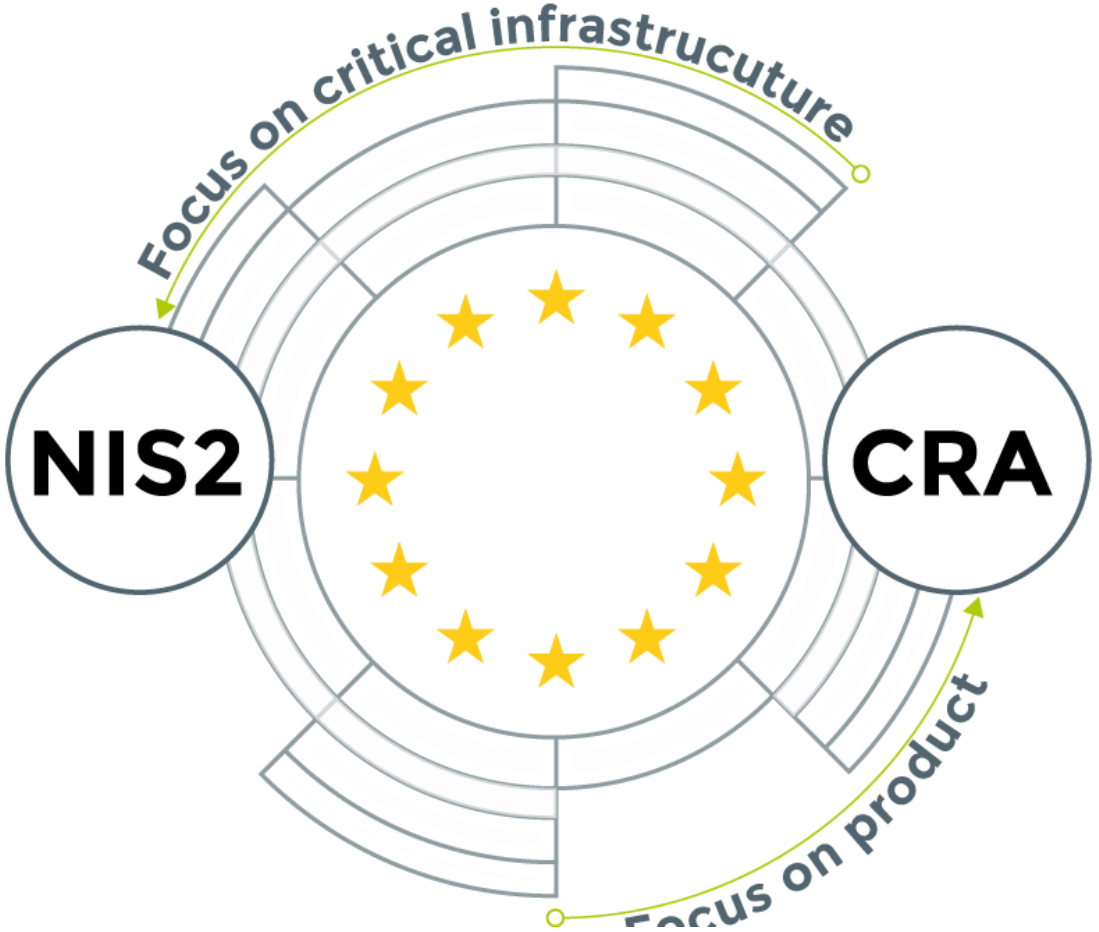
Christoph Schmittner

Christoph.schmittner@ait.ac.at

SYNERGIE ZWISCHEN CRA UND NIS2

- **Zielgruppen**:
  - **NIS2**: Organisationen
  - **CRA**: Produkte mit digitalen Elementen, die auf dem EU-Markt verkauft werden

- **Anforderungen**:
  - **NIS2**: Sicherheitsmaßnahmen, Governance-Strukturen, Vorfallmeldungen und Lieferkettenüberwachung für Organisationen
  - **CRA**: Sicherheitsanforderungen für Produkte, regelmäßige Sicherheitsupdates, Schwachstellenmanagement und Cyber-Risikobewertung vor Markteinführung



KLASSE I+II: HARMONISIERTE STANDARDS

Ein harmonisierter Standard ist ein Standard, der von der Europäischen Union anerkannt wird und die Einhaltung rechtlicher Anforderungen erleichtert.

Bedeutung im Kontext des CRA

Produkte, die mit harmonisierten Standards übereinstimmen, gelten als konform mit den wesentlichen Anforderungen der CRA-Verordnung.

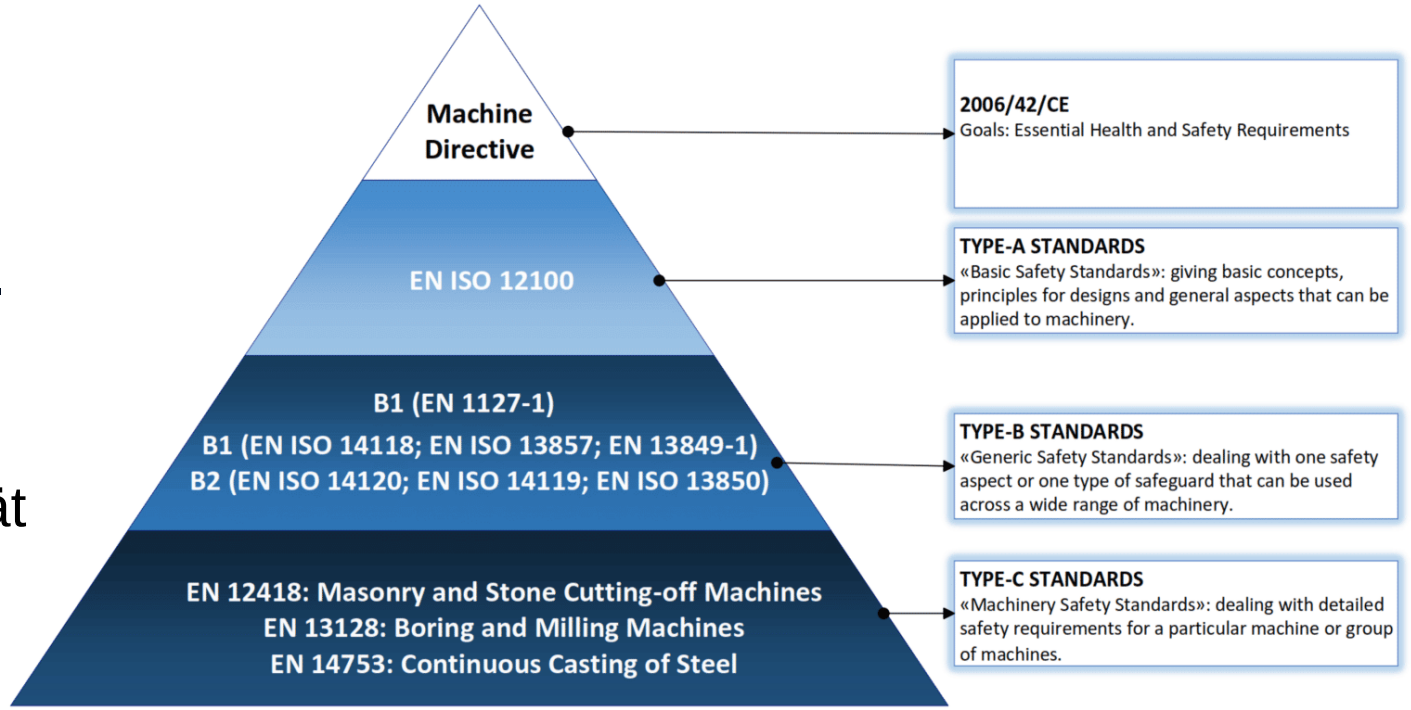
Harmonisierte Standards werden gemäß der EU-Verordnung Nr. 1025/2012 entwickelt

Entwicklung basierend auf IEC 62443

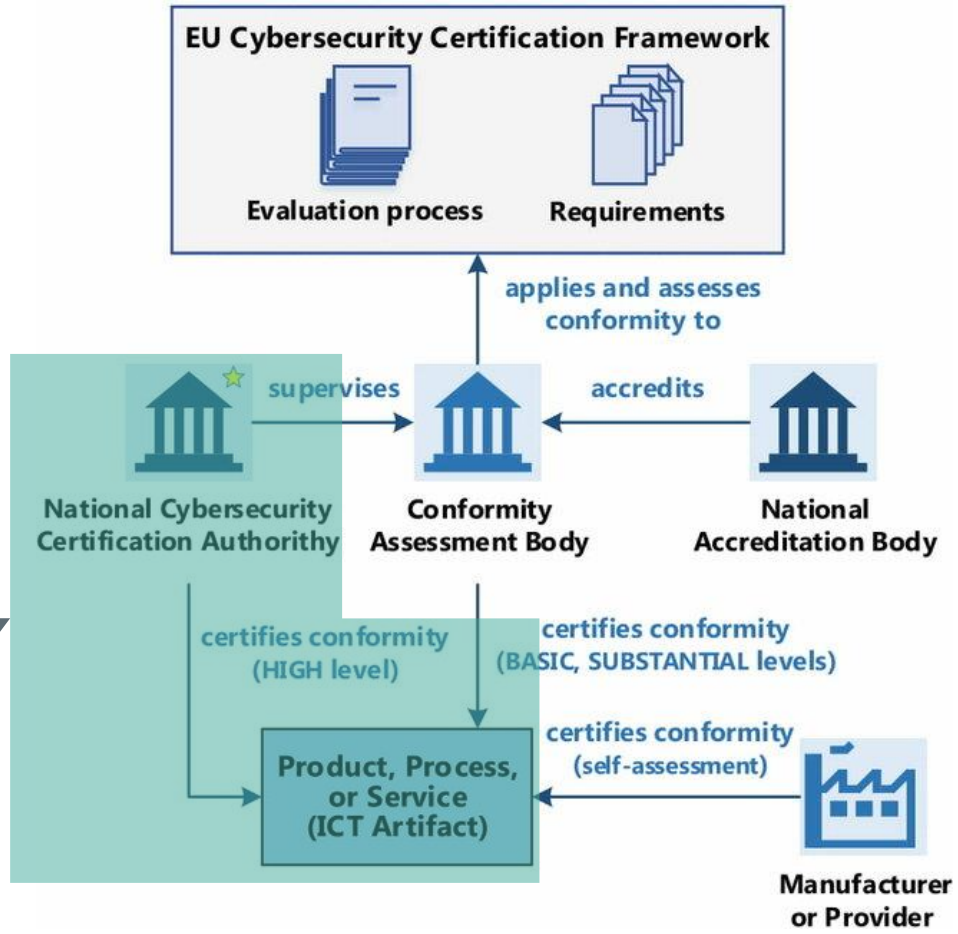
Basierend auf z.B. der IEC 62443 werden derzeit harmonisierter Standards für ICT-Komponenten entwickelt

KLASSE I+II: HARMONISIERTE STANDARDS

- Entwicklung durch eine europäische SDO, auf Basis einer Anfrage der Europäischen Kommission
  - CEN, CENELEC, ETSI
- Harmonisierte Normen sind optional.
  - Befolgung führt zur Annahme der Konformität.
  - Ohne Befolgung muss Konformität selbst nachgewiesen werden.
- 30/10/2026 gesetzte Deadline



EUROPEAN CYBERSECURITY CERTIFICATION SCHEME FOR CRITICAL PRODUCTS



Kritische Produkte mit digitalen Elementen (basierend auf aktuellem Text)