Einführung in den CRA

Regulation on horizontal cybersecurity requirements for products with digital elements

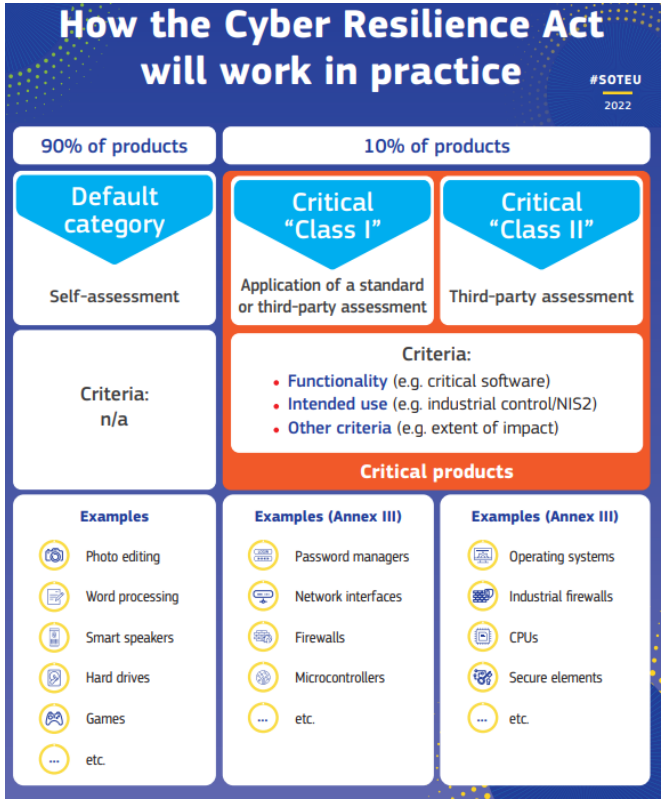
Prof. Dr. Dennis-Kenji Kipker, DKE

DKE

Rechtspolitischer und systematischer Hintergrund

- Stärkung der **horizontalen Cybersecurity** auf EU-Ebene schon lange Thema/von Branchenverbänden als bislang unzureichend kritisiert → vgl. Diskussion um EU CSA (2019)
- Verbesserte Anschlussfähigkeit an **New Legislative Framework (NLF)** zu gewährleisten
- Horizontale Regelungen sollen vertikalen und produktgruppenspezifischen Rechtsakten vorgezogen werden → Ziel: **Verhinderung von Fragmentierung/mehr Kohärenz** in Anforderungen

Systematische Zusammenhänge und Produktrisiken



- **Kommissionsentwurf** vorgestellt Mitte September 2022
- Die **„Spinne im Netz“**: Umfassende Bezugspunkte zu weiteren EU-Rechtsakten (z.B. NIS-2, AIA, CSA, MaschinenVO)
- Besonders restriktive **Marktüberwachungsanforderungen** für Produkte mit erheblichem Cybersicherheitsrisiko
- **Abgrenzungsfragen:**
  - **NIS-2:** Unternehmensbezogene Richtlinie
  - **CRA:** Produktbezogene Verordnung

Quelle: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet

Überblick über die Anforderungen im Einzelnen

1.	2.	3.	4.	5.
Produkte mit digitalen Elementen (Hardware/Software)	**„Security by Design“ als Lebenszyklus-anforderung (EoL)**	**Risikobewertung und Dokumentations-pflichten**	**Schutz der Lieferkette unter Einbeziehung von Produkten aus Drittstaaten**	**Pflicht zu Sicherheits-aktualisierungen „by default“**

Produkte mit digitalen Elementen

- Bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung umfasst eine direkte oder indirekte logische oder physische Datenverbindung zu einem Gerät oder Netz
- Jedes Software- oder Hardwareprodukt und mit ihm verbundene Cloudlösungen
- Separat in Verkehr gebrachte Software- und Hardware-Komponenten
- → **Weit gefasster Anwendungsbereich**

Cybersecurity als Anforderung „by design“: Hersteller

- **Risikobewertung** für Entwurf, Entwicklung, Herstellung, Lieferung und Wartung von Produkten
- **Digitale Lieferkette:** Komponenten von Drittherstellern dürfen Cybersecurity des Endprodukts nicht kompromittieren
- **Dokumentationspflicht** + Verbraucherinformation
- **Korrekturmaßnahmen** bei fehlender/unzureichender Cybersecurity bis hin zu Rücknahme/Rückruf
- **Meldungen** ggü. ENISA unverzüglich/innerhalb von 24 Stunden nach Kenntniserlangung für aktiv ausgenutzte Sicherheitslücken

Cybersecurity als Anforderung „by design“: Importeure und Händler

- **Importeure:**
  - „Importeur“: Jede in der Union ansässige natürliche oder juristische Person, die ein Produkt mit digitalen Elementen in Verkehr bringt, das den Namen oder die Marke einer außerhalb der Union ansässigen natürlichen oder juristischen Person trägt
  - Nur Inverkehrgabe von Produkten mit CRA-Konformität
  - Anforderungen mit Hersteller vergleichbar, zusätzliche Informationspflichten (insb. Kontaktangaben)
  - Bei Nichtentsprechung mit CRA Rücknahme/Rückruf
  - Bei Schwachstellen Information an zuständige mitgliedstaatliche Marktüberwachungsbehörden
- **Händler:** Vergleichbare Anforderungen wie Importeure im Hinblick auf Konformität mit CRA

Sanktionen und Bußgelder

- **Bei unzureichendem Tätigwerden bzw. Nichttätigwerden des Herstellers:** Untersagung des Produktvertriebs möglich
- **EU:** „wirksame, verhältnismäßige und abschreckende“ Sanktionen
- **Legislativer Vorschlag zur Bebußbarkeit von Verstößen** gegen grundlegende Cybersicherheitsanforderungen:
  - Maximal 15.000.000 EUR oder wenn es sich bei dem Zuwiderhandelnden um ein Unternehmen handelt, in Höhe von bis zu 2,5 % seines gesamten weltweiten Jahresumsatzes im vorausgegangenen Geschäftsjahr
  - Geringfügigere Verstöße abgestuft beginnend mit 5.000.000 EUR bzw. 1% des im vorausgegangenen Geschäftsjahr erzielten weltweiten Gesamtjahresumsatzes
  - **Mehrfachbebußung** für dieselbe Zuwiderhandlung nicht ausgeschlossen