

TeleTrust "IT-Sicherheitsrechtstag 2023"

Berlin, 28.09.2023

EU Cyber Resilience Act (CRA)

RA Dr. Christoph Bausewein CIPT

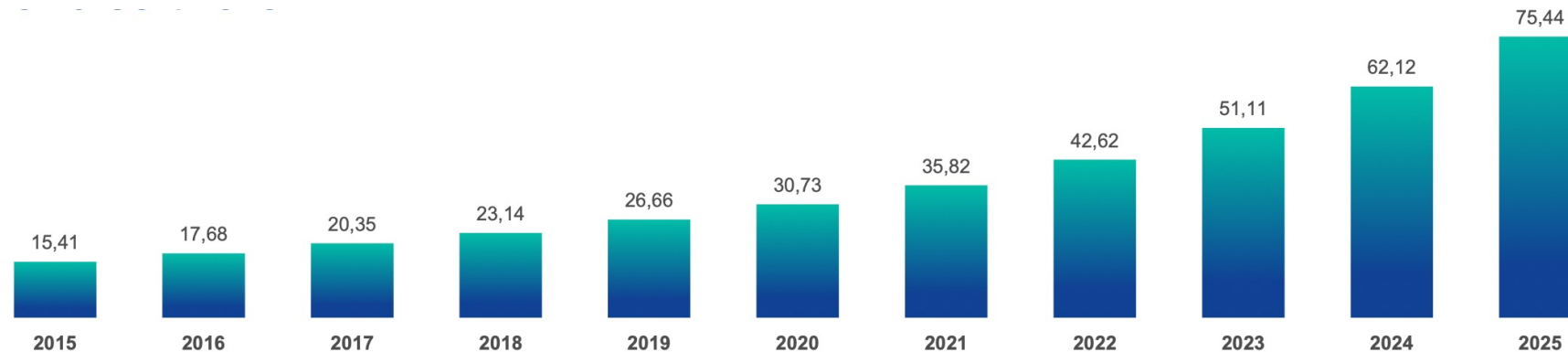
Assistant General Counsel, Data Protection & Policy, CrowdStrike

If everything is connected, everything can be hacked.

Ursula van der Leyen

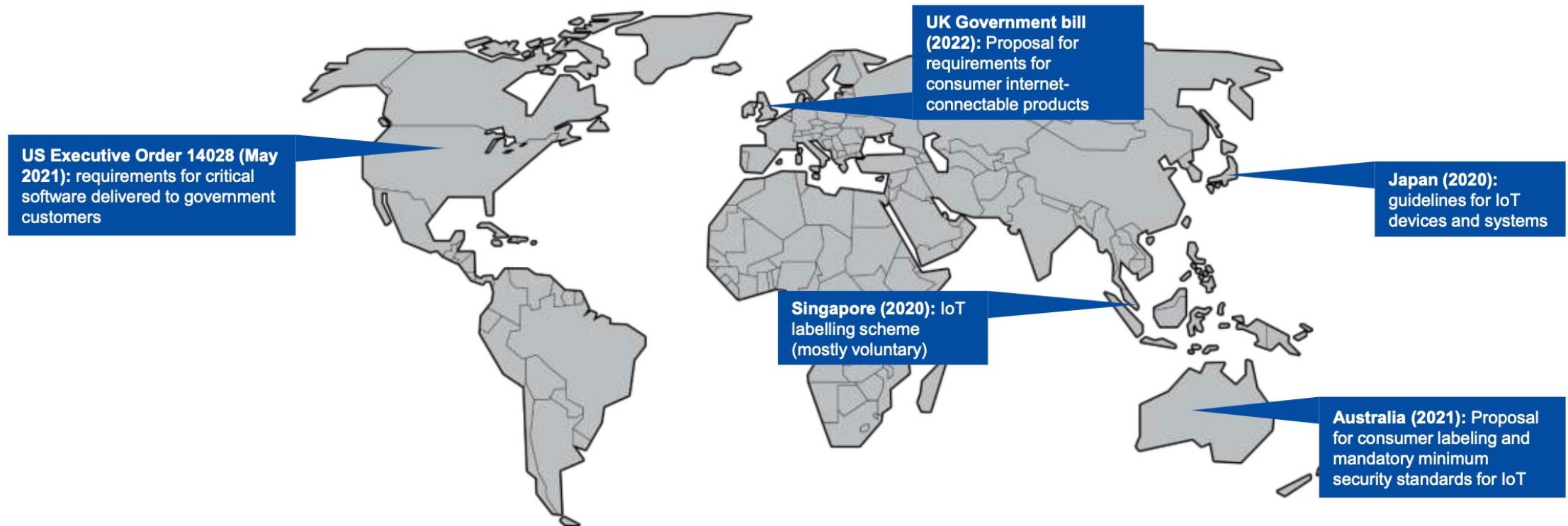
Regelungsgrund

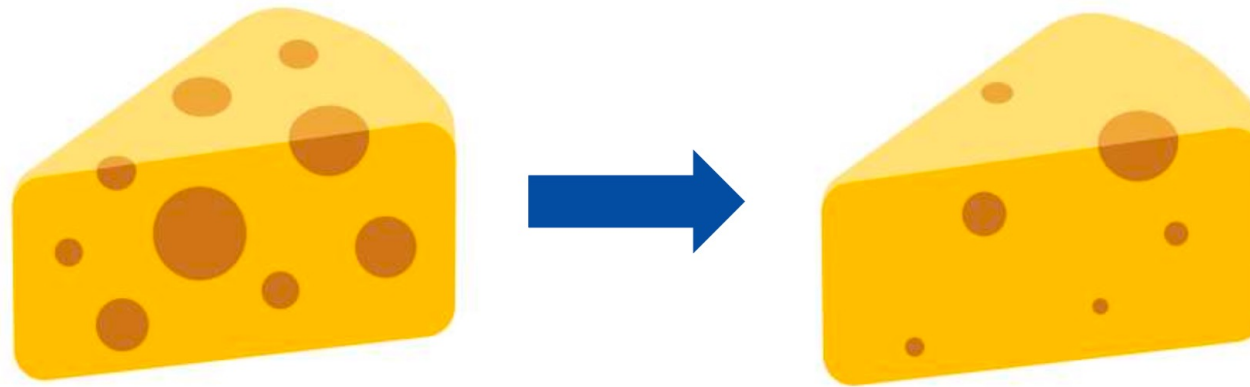
- Anteil an Internet of Things (IoT) Geräten steigt stetig
- IoT-Schwachstellen können über das Internet ausgenutzt werden
- Hersteller, Verkäufer oder Importeure von IoT-Geräten haben nur schwache Anreize für sichere Hardware und Software zu sorgen



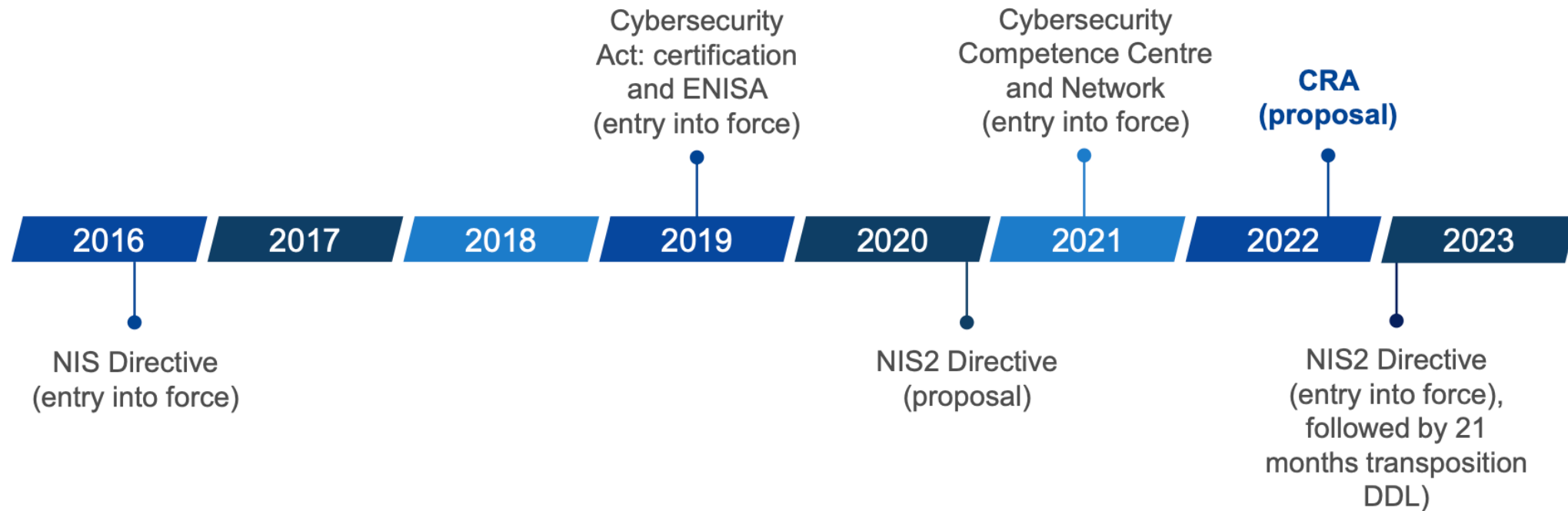
Internet of Things devices worldwide from 2015 to 2025 (in billions)

Source: Forbes/IHS





Wie die Löcher aus dem Käse ziehen?



Käselochschließung à la Europäischer Kommission

- Vernetzte Produkte sollen sicherer werden, indem Hersteller, Verkäufer und Importeure vernetzter Produkte bzw. deren Software zu Folgendem verpflichtet werden:
 - **Security by Design** – Maßnahmen inkl. Schwachstellenmanagement während des gesamten Produktlebenszyklus bzw. mindestens 5 Jahre
 - Risikobasierter **Konformitätserklärung**
 - **Meldung von Sicherheitsvorfällen** oder aktiv ausgenutzten Sicherheitslücken unverzüglich nach Bekanntwerden bei der zuständigen Behörden

Konformitätsprüfung à la Europäischer Kommission

- **Produkte mit durchschnittlichem Risiko** (~90%): Selbstbewertung (Beispiele: Fotobearbeitung, Textverarbeitung, intelligente Lautsprecher, Festplatten, Spiele usw.)
- **Kritische Produkte** (~10%): Explizit benannte Produkte (Beispiele: Firewalls, CPUs, Betriebssysteme usw.) müssen besonderes Konformitätsbewertungsverfahren durch einen unabhängigen Dritten durchlaufen
- **Hochkritische Produkte**: obligatorische Zertifizierung auf der Grundlage von EU-Zertifizierungssystemen für Cybersicherheit (CSA) notwendig

■ Produkte mit digitalen Elementen

- Hardware
- Software

■ NICHT im Anwendungsbereich

- Services incl. IaaS, SaaS (covered by NIS2)
- Produkte mit digitalen Elementen, die lex speciales unterfallen (z.B. Auto, medizinische Geräte)
- Nicht kommerzielle Open Source Software

Käselochschließung à la Europäischem Parlament (ITRE)

- Cybersicherheit-Mindeststandards für Produkte des täglichen Lebens mit digitalen Elementen (inkl. Türklingeln, Videokameras für den privaten Gebrauch, Babyphone, Wi-Fi-Router, Identity Management Systems Software, Passwortmanager, Biometrische Lesegeräte, Smart Home Assistenten, Smartwatches)
- Automatische Sicherheitspatches (wenn technisch möglich)

Käselochschließung à la Rat der EU

- Verbindliche Cybersicherheitsanforderungen für die **Konzeption, Entwicklung, Herstellung** und das Inverkehrbringen von Hardware- und Softwareprodukten
- Produkte, die **direkt oder indirekt** mit einem anderen Gerät oder einem Netz verbunden sind (z. B. Medizinprodukte, Luftfahrt- und Kraftfahrzeuge, intelligente Kühlschränke, Smart-TVs, and -Spielzeuge)
- Pflicht zur **Bewertung** der Cybersicherheitsrisiken
- Pflicht zur **Zusammenarbeit** mit den zuständigen Behörden

Zusammenspiel mit anderen EU Rechtsakten

- Allgemeine Produktsicherheitsverordnung / General Product Safety Regulation (GSPR) (ersetzt ab 13.12.2024 die aktuelle General Product Safety Richtlinie und die Food Imitating Product Richtlinie)
- Verordnung (EU) 2023/1230 zum Maschinenbau (ersetzt Richtlinie 2006/42/EC)
- AI Act
- Delegated Act on the RED → the CRA replaces the delegated act of the RED (explanatory memorandum – interplay with other Union policies)
- Cybersecurity Act
- NIS 2

Sanktionsmittel à la Europäischer Kommission

- Aufforderung zur Beseitigung der Nichtkonformität bzw. des Risikos
- Produktrückruf
- Einschränkung von Herstellung, Vertrieb und Import des Produkts
- Sanktionen einschließlich Geldbußen bis zu 15 Mio. EUR oder bis zu 2,5 % des weltweiten Umsatzes

- **Innovationsbremse**
- **Bürokratischer Aufwand** durch Pflicht zur selbständigen Konformitätsprüfung und Meldepflichten
- **Überregulierung** (überzogener Anwendungsbereich)
- Blockade von **Open-Source-Projekte** mit geringem finanziellen und personellen Ressourcen und damit einhergehende Probleme für die IT-Branche, wenn Open-Source-Komponenten wegfallen
- **Rechtsunsicherheit** durch unbestimmte Rechtsbegriffe