Cyber Resilience Act

Cyberresilienz für Produkte mit digitalen Elementen

Mag. Verena Becker, BSc
Bundessparte Information und Consulting/Wirtschaftskammer Österreich

4. November 2024

Vorstellung Mag. Verena Becker, BSc (WU)

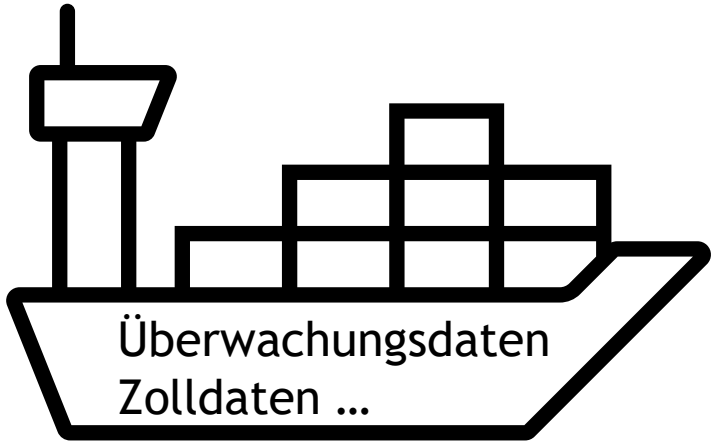
- Cybersicherheitsexpertin in der Bundessparte Information und Consulting/WKÖ
- Cofounderin des Frauennetzwerks Women4Cyber Austria
- Juristin und Betriebswirtin
- Information Security Managerin und Senior Risk Managerin
- Wirtschaftstrainerin

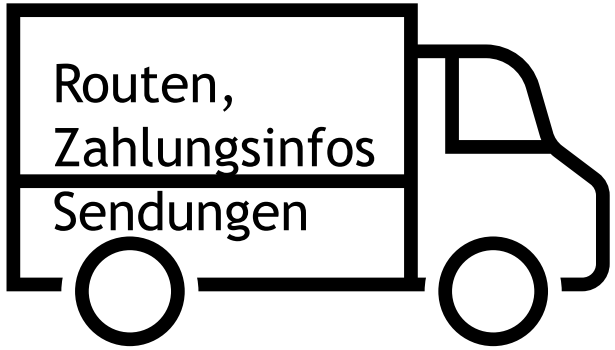
Ziele des Cyber Resilience Act

- Erhöhung Cyberresilienz und Transparenz für Hard- und Software
- besserer Schutz für gewerbliche Nutzer und Verbraucher
- gilt für alle Produkte mit digitalen Element,
die in der EU auf den Markt gebracht werden
- EU-weiter einheitlicher Rechtsrahmen

Cyberresilienz am Beispiel Transportwirtschaft

- Sicherheit und Resilienz digitaler Systeme hochrelevant
- Einfluss auf Gesamtwirtschaft
- Abhängigkeit von komplexen Lieferketten
- große Datenmengen

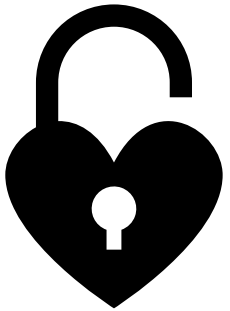




Der Cyber Resilience Act soll

- sicherstellen, dass Hard- und Software **weniger Schwachstellen** aufweist

- sicherstellen, dass Hersteller während **gesamten** **Lebenszyklus** des Produkts verantwortlich bleiben



- **Transparenz** in Bezug auf Sicherheit verbessern

- besseren **Schutz für gewerbliche Nutzer und Verbraucher** gewährleisten

Pflichten

- Sicherheitsanforderungen an die Eigenschaften digitaler Produkte, z.B. Security by Design, Security-by-Default
- Anforderungen an Umgang mit Schwachstellen
- Meldepflichten
- Transparenz

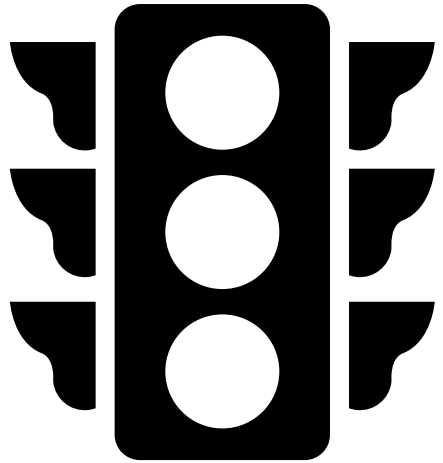
→ Pflichten für Hersteller, Händler und Importeure

Klassifikation je nach Risikoniveau

- Standardkategorie: ca. 90% der Hard- und Software

- wichtige Produkte:
  - wichtige Produkte Klasse 1
  - wichtige Produkte Klasse 2

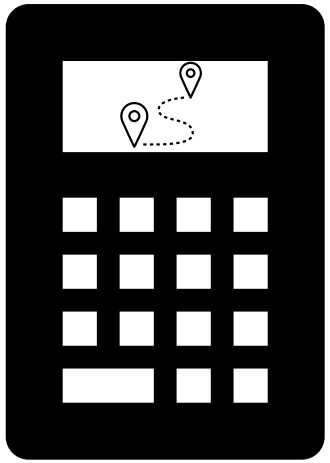
- kritische Produkte



Beispiel Steuerungssystem mit Computer-Chip

Hersteller muss

- Einhaltung von Cybersicherheitsnormen bei Entwicklung und Produktion nachweisen
- Dokumentation über Software-Stückliste
- Konformitätsbewertungsverfahren: CE-Kennzeichen
- für Chip und Steuerungssystem Updates, Melde- und Informationspflichten



Zeitplan

- **Q4/2024**: Veröffentlichung im EU-Amtsblatt
  → 20 Tage nach Veröffentlichung Inkrafttreten

- **September(?) 2026**: Meldepflichten für Hersteller in Bezug auf aktiv ausgenutzte Schwachstellen und Sicherheitsvorfälle (21 Monate nach Inkrafttreten)

- **Q4/2027**: volle Anwendung (36 Monate nach Inkrafttreten)

Wo bekomme ich Unterstützung

- Förderungen: KMU DIGITAL
- Informationen zum Cyber Resilience Act – https://wko.at/cra
- Informationen zu NIS2 - https://wko.at/nis2
- Schulungen zum Cyber Resilience Act und NIS2 – https://incite.at
- Informationen zu Cybersicherheit – https://it-safe.at
- Suche nach IT-Security-Expert: innen

Mag. Verena Becker, BSc

Bundessparte Information und Consulting
Wirtschaftskammer Österreich
T 05 90 900-3176
E verena.becker@wko.at
W https://wko.at/cra
W https://it-safe.at | W https://wko.at/nis2