Cyber Resilience Act und Ich
Was bedeutet der CRA für Mich?

Lars Francke -
https://stackable.tech

Cyber Resilience Act / Disclaimer

Dieser Talk bezieht sich auf die öffentliche Version des CRA vom 31. August 2023

https://data.consilium.europa.eu/doc/document/ST-12536-2023-INIT/en/pdf

- Es gibt verschiedene Versionen verschiedener EU Gremien
  - diese ist bisher die sinnvollste in Sachen FOSS
- Es kann sich noch einiges ändern
  - bzw. es hat sich hinter verschlossenen Türen schon wieder etwas geändert
- Ich bin kein Anwalt und sowieso ist hier nichts als Ratschlag oder Rechtsberatung zu verstehen sondern nur meine eigene Interpretation der Dinge
  - Ich bin auch kein Experte sondern in das Thema reingerutscht
- Verklagt mich nicht!

Stackable

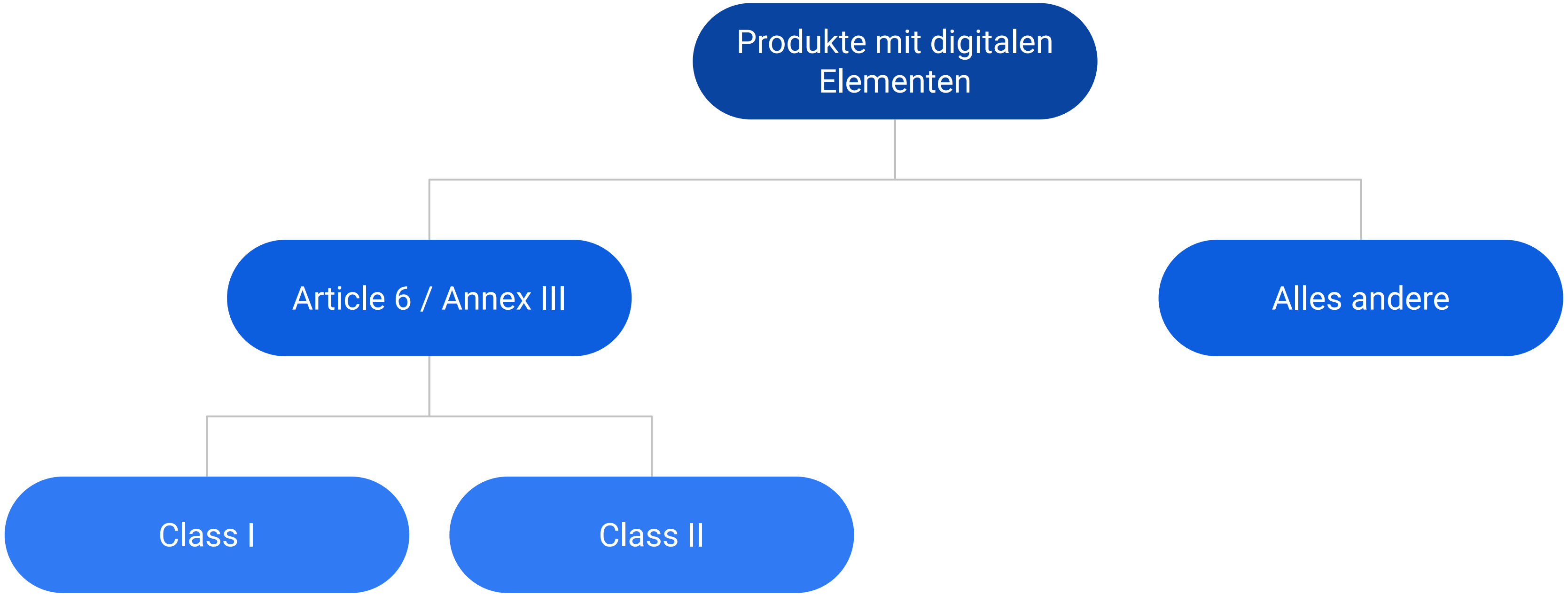
Frage 1: Bin ich betroffen

Für diesen Talk: JA!

Sind wir nicht alle ein bisschen “**manufacturer**”, “**importer**” oder “**distributor**”?

Kurz: “**economic operator**”

Frage 2: Was bin ich?



Class I:

- Boot Loader
- Malware / Antivirus scanner
- Betriebssysteme
- ...

Class II:

- VPN Server & Clients
- Container Runtime Systems (Kubernetes) & Hypervisor
- Firewalls, IDS etc.

Frage 2: Was muss ich tun um ein Produkt überhaupt veröffentlichen zu dürfen?

Ihr habt gefragt!

Stackable

CRA: Schritte zur Konformität

Schritt 1: CE marking (Article 22)

CE Zeichen / Article 22

Kurz gesagt:

CRA:

✅

CRA: Schritte zur Konformität

Schritt 1: EU Declaration of conformity (Article 20/24)

Schritt ~~1~~2: CE marking (Article 22) ✅

EU Declaration of conformity (Article 20, 24, Annex IV)

- Name und Typ des Produktes (zur eindeutigen Identifikation)
- Name und Adresse des Herstellers (oder Vertreter)
- Statements, dass
    - man selber verantwortlich ist für die declaration
    - das man alle relevanten Regeln beachtet hat
    - dass das genannte Produkt den Regeln des CRA entspricht
- Wo nötig (Class I / Class II) Name und Nummer der zertifizierenden Stelle

EU DECLARATION OF CONFORMITY

The EU declaration of conformity referred to in Article 20, shall contain all of the following information:

1. Name and type and any additional information enabling the unique identification of the product with digital elements;
2. Name and address of the manufacturer or his authorised representative;
3. A statement that the EU declaration of conformity is issued under the sole responsibility of the provider;
4. Object of the declaration (identification of the product allowing traceability. It may include a photograph, where appropriate);
5. A statement that the object of the declaration described above is in conformity with the relevant Union harmonisation legislation;
6. References to any relevant harmonised standards used or any other common specification or cybersecurity certification in relation to which conformity is declared;
7. Where applicable, the name and number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued;
8. Additional information:

   Signed for and on behalf of: ……………………………….

   (place and date of issue):

   (name, function) (signature):

Conformity Assessment? Conformity Assessment! (Annex VI)

Internal control procedure

- Alles was nicht Class I / Class II oder sonst wie speziell ist
    - Dürfte auf den Großteil an Software zutreffen
- Ohne Drittparteien
- Eigenbestätigung, dass man alle Anforderungen erfüllt

EU-type examination

- “Notified body” führt das Assessment durch
- Von der EU “zertifizierte” Stelle

Internal production control & Full quality assurance

- Habe ich mir nicht weiter angeguckt…

CRA: Schritte zur Konformität

Schritt 1: Dokumentation (Article 23)

Schritt ~~1~~2: EU Declaration of conformity (Article 20/24) ✅

Schritt ~~2~~3: CE marking (Article 22) ✅

Stackable

Dokumentation / Article 23 / Annex V

- Dokumentation des Risk Assessment
- Muss zur Veröffentlichung des Produkts fertig sein und aktuell gehalten werden
- Beschreibung der Software, inkl. Versionen und Compliance Status
- Beschreibung des Design, Entwicklungs und Herstellungsprozesses inklusive Schwachstellenmanagement
  - inkl. Zeichnungen, Architektur, Zusammenhänge zwischen Komponenten
- Links zu SBOMs, Vulnerability Disclosure Policy, Kontaktadresse für Schwachstellen
  - Software Bill of Materials (SBOM)
    - Standardisiert (aktuell wohl CycloneDX oder SPDX) und manschinenlesbar
    - mindestens die top-level Abhängigkeiten
    - Siehe dazu auch BSI TR-03183 Teil 2
- Beschreibung des Updateverfahrens
- Beschreibung wie alle obigen Prozesse sichergestellt und überwacht werden
- Beschreibung von Tests, die gemacht wurden
- Kopie der EU declaration of conformity
- 10 Jahre aufbewahren

Stackable

CRA: Schritte zur Konformität

Schritt 1: Risk Assessment

Schritt ~~1~~2: Dokumentation (Article 23) ✅

Schritt ~~2~~3: EU Declaration of conformity (Article 20/24) ✅

Schritt ~~3~~4: CE marking (Article 22) ✅

Stackable

Risk Assessment

Article 10

Obligations of manufacturers

1. When placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential requirements set out in Section 1 of Annex I.

ANNEX I

<u>ESSENTIAL CYBERSECURITY REQUIREMENTS</u>

1. SECURITY REQUIREMENTS RELATING TO THE PROPERTIES OF PRODUCTS WITH DIGITAL ELEMENTS

Risk Assessment

- Bewertung der Cybersecurity Risiken eines Produkts nach Annex I Section 1
- Ergebnis muss einfließen in Design, Entwicklung, Produktion, Lieferung und Wartung
- Die Bewertung muss während der gesamten erwarteten Lebensdauer eines Produkts aktuell gehalten werden
- Muss Begründung beinhalten falls gewisse Punkte nicht relevant sind
- Die Bewertung muss Teil der technischen Dokumentation sein (Article 23 / Annex V)

Annex I: Essential Cybersecurity Requirements

Dinge, die man noch halbwegs vernünftig machen kann:

- Keine bekannten ausnutzbaren Schwachstellen (known exploitable vulnerabilities)
- Sichere Default Konfiguration
- Auto Update oder mindestens Benachrichtigung über Updates (Phone Home), Opt Out
- Autorisierung / Authentifizierung
- Encryption on-the-wire & at-rest
    - Confidentiality, Integrity (keine Manipulation von Daten)
- Datenminimalismus (Privacy)
- Audit Funktionalität
- Möglichkeit zum Löschen aller Daten

Und dann ein paar schwammige Dinge:

- Schutz essentieller Funktionen (uhm….) z.B. gegen DDoS Angriffe
- "Minimise the negative impact by themselves or connected devices on the availability of services provided by other devices or networks"
- Angriffsoberfläche minimieren
- Auswirkung von Angriffen minimieren

Stackable

CRA: Schritte zur Konformität

Schritt 1: Risk Assessment ✅

Schritt 2: Dokumentation (Article 23) ✅

Schritt 3: EU Declaration of conformity (Article 20/24) ✅

Schritt 4: CE marking (Article 22) ✅

Stackable

Produkt veröffentlicht. Was nun?

https://www.pexels.com/photo/flight-sky-earth-space-2159/

Nach der Veröffentlichung.....ist vor der Veröffentlichung

- Die ganze Prozedur muss erneut für jede neue Version durchgeführt werden
- Security Updates müssen geliefert werden
- Dokumentation und Bewertungen müssen aufrecht erhalten werden
- End-of-Life Datum muss mit Jahr und Monat angegeben werden
  - Definition der Produktlebensdauer darf nicht willkürlich sondern wie sie ein Benutzer vernünftigerweise erwarten würde
- Bis dahin muss man “compliant” bleiben oder Produkt zurückrufen
- Im Falle einer Insolvenz: Behörden informieren

Stackable

Annex I - Section 2: Vulnerability Handling Requirements

- Alle Schwachstellen müssen dokumentiert werden und effektiv behandelt werden
  - Während der gesamten Produktlebensdauer
  - z.B. durch Updates
- Regelmäßige Tests und Security Reviews
- Public Disclosure von Schwachstellen inkl. Informationen zu Mitigation usw.
  - Für eigene und third-party Komponenten
  - VEX Statements
- Policy zu Coordinated Vulnerability Disclosure

Schwachstellenmanagement / Updates

- Es reicht die letzte Version zu unterstützen solange Nutzer kostenlosen Zugriff darauf haben und es keine signifikanten zusätzlichen Kosten gibt um darauf zu aktualisieren
- Alte Versionen dürfen weiter abrufbar sein solange man klar auf die Risiken hinweist
  - Das wird noch spannend mit Dingen, die automatisch abgerufen werden
- Fixes müssen kostenlos upstream zur Verfügung gestellt werden
- Innerhalb von 24 Stunden müssen Behörden (ENISA) über “actively exploited vulnerabilities” und “incidents having an impact on the security of the product” informiert werden
- Follow-up sobald mehr Informationen dazu kommen
- Und mehr…
- Kommt nicht gut an: Behörden exklusiven Zugriff auf Schwachstellen geben
  - Was kann da schief gehen?
- Informationen über Schwachstellen in maschinenlesbarer Form
  - z.B. CSAF

Stackable

Vielen Dank

Kontakt

Lars Francke
lars.francke@stackable.tech
https://www.linkedin.com/in/larsfrancke/
+49 (172) 4554978

Stackable