

EU Cyber Resilience Act: Fakten, Mythen und Ungeklärtes

CRA = Cyber Resilience Act

- Verordnung – gilt ab Beschluss (Dezember 2024)
- Vollkommen aktiv ab Dezember 2027
- Meldepflichten für Hersteller schon ab September 2026
- Ziele: Hersteller in die Pflicht nehmen, Cybersicherheit von Produkten in der EU stärken

Hintergrund

It's a Sequel!

Mythbusting CRA: Nicht alle Gerüchte über den
Cyber Resilience Act sind wahr

FEATURED | VERBANDS-NEWS | 20. FEBRUAR 2025



Wichtige Definitionen

Produkt mit digitalen Elementen (PDE)

Hersteller

Open-source software stewards (Verwalter quelloffener Software)

SBOM

Produkt mit digitalen Elementen

ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in den Verkehr gebracht werden

Hersteller

eine natürliche oder juristische Person, die Produkte mit digitalen Elementen entwickelt oder herstellt oder die Produkte mit digitalen Elementen konzipieren, entwickeln oder herstellen lässt und sie unter ihrem Namen oder ihrer Marke vermarktet, sei es gegen Bezahlung, zur Monetarisierung oder unentgeltlich;

Open-source software stewards


eine juristische Person, bei der es sich nicht um einen Hersteller handelt, die den Zweck oder das Ziel hat, die Entwicklung spezifischer Produkte mit digitalen Elementen, die als freie und quelloffene Software gelten und für kommerzielle Tätigkeiten bestimmt sind, systematisch und nachhaltig zu unterstützen, und die die Brauchbarkeit dieser Produkte sicherstellt;

SBOM

Software
Bill
Of
Materials

Format zum Dokumentieren von
Abhängigkeiten (und Informationen über
diese)

Mythos 1



“Mein Open Source Projekt
verlangt CRA-Conformity
wenn es von anderen
geschäftlich genutzt wird”

Mythos 1

“*Mein Open Source Programm* verlangt CRA-Conformity wenn es von anderen geschäftlich genutzt wird”

Solange das Produkt nicht kommerziell ist, fällt es nicht unter den CRA (Artikel 3 (13&14))

Public Service Announcement


**HOBBY SOFTWARE, DIE KEIN KOMMERZIELLES ZIEL
VERFOLGT FÄLLT AUßERHALB DES CRA'S**

Mythos 2

“Meine Open Source Library
verlangt CRA-Conformity
wenn es von anderen
geschäftlich genutzt wird”

Nein! Die CRA-Konformität liegt immer an der Entität, welche das Produkt auf den EU-Markt bringt. Dem Hersteller ist Sorgfalt bei der Auswahl von Dependencies abverlangt (Art. 13 Abs. 5)

Mythos 3



“Eine SBOM muss
mindestens X Dependencies
tief sein”

Nein, es müssen nur die
obersten Dependencies
eingetragen werden (Anhang I
Teil II (1))*

***Zu beachten: BSI TR-03183-2 verlangt z.B. im Delivery Item SBOM mehr.**

Mythos 4

“Als Open Source Projekt, muss ich jedes Release mindestens für 5 Jahre mit Sicherheitsupdates versehen”

Nein!

Die 5-Jahres-Support-Periode bezieht sich auf Hersteller von PDEs (Art. 13 Abs. 3/8). Dort muss nur die aktuellste Version unterstützt werden sofern Nutzer die Möglichkeit haben ohne Kosten zu aktualisieren (Art. 13 Abs. 10)

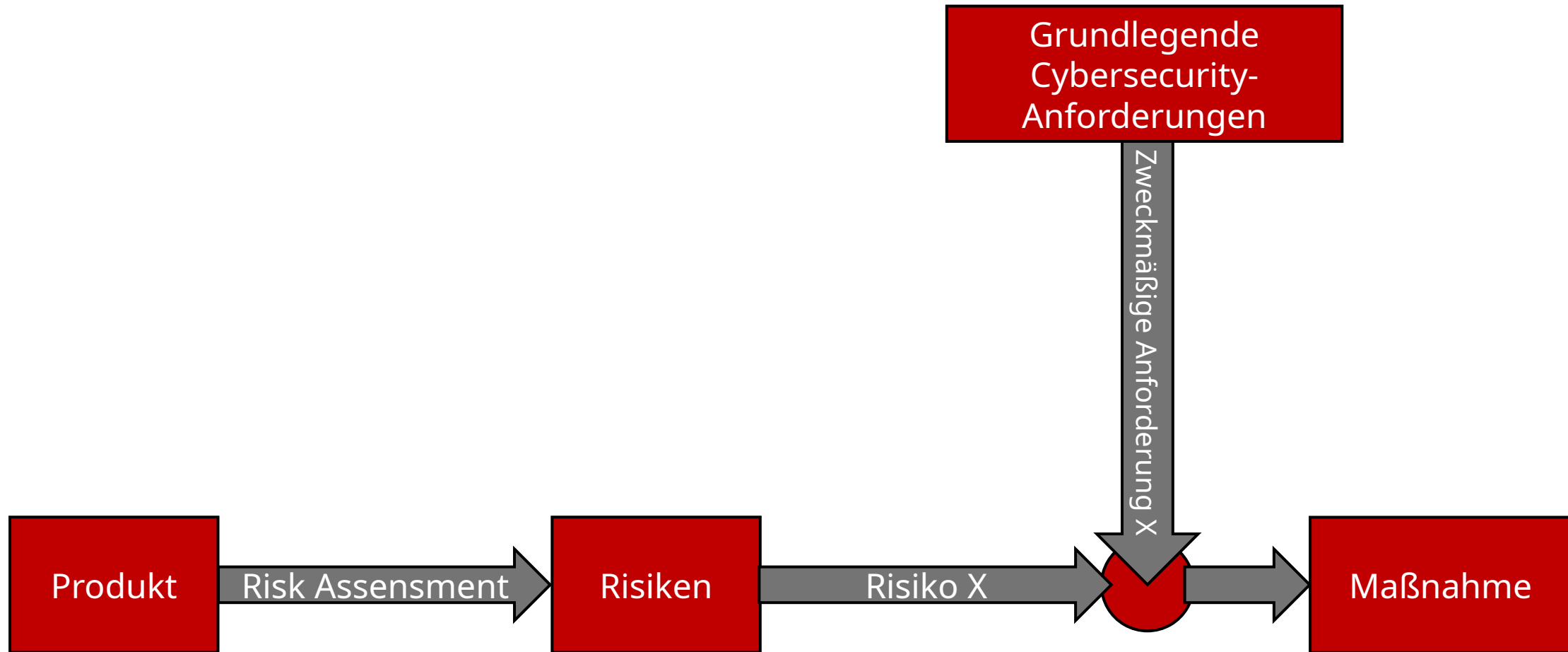
Mythos 5



“Ich brauche UNBEDINGT
Sicherheitsfeature X, egal
was das Produkt ist”

Nein!
Sicherheitsfeatures müssen “Auf der
Grundlage der Bewertung der
Cybersicherheitsrisiken”
implementiert werden (Anhang I Teil
I (2))

Mythos 4



Grundlegende Cybersecurityanforderungen lassen sich in Anhang I Teil I finden.

Ungeklärtes

- Es fehlen genauere Infos (ab wann ist etwas kommerziell?)
→ Maarten Aertsen zu Monetarisierung [1]
- Wie werde ich ein Steward?
- Anlaufstellen?
- Schematas?

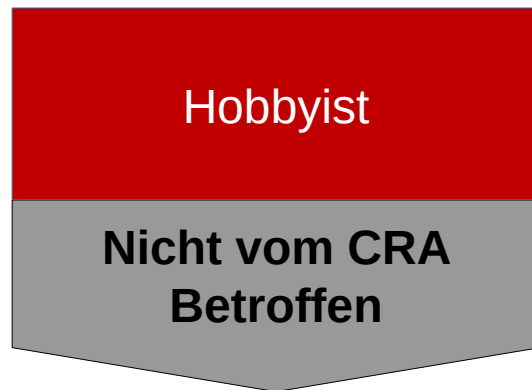


Tipps für den Weg

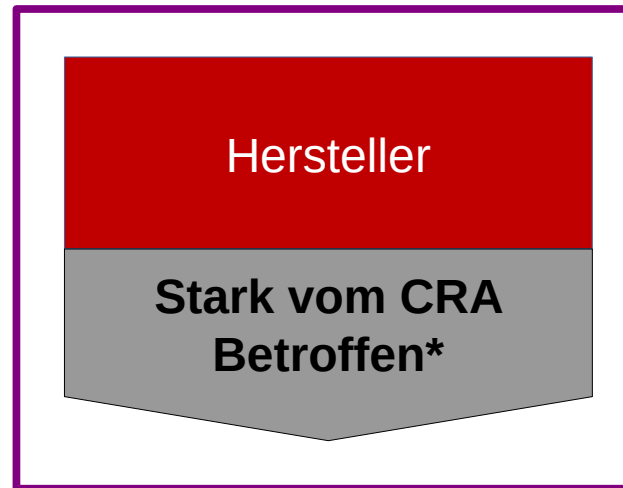
- Dokumentiert die komplette Entwicklung des PDEs
- Lasst euch als Hobbyist nichts aufschwätzen
- Zwingt euch keine Rollen auf
- Vage Formulierungen geben Spielraum
- Ausschau nach Guidance halten

Fazit

non-kommerziell



kommerziell



*Risk Assessment machen, um zu sehen wie schlimm es ist

Mehr Infos?



**CRA in allen
Sprachen**



**Webinar Benjamin
Bögel &
Eclipse foundation**

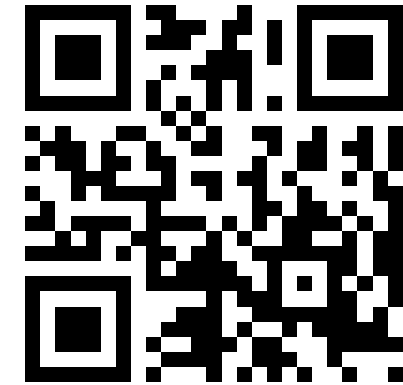


**Mythbusting
Teil 1**

Fragen?



Sprecht mich an!



Schreibt mir ne mail!

`samuel.precupas@sodgeist.de`

Externe Quellen

[1] <https://www.linkedin.com/events/7326102296910573568/> , 28:17, Maarten Aertsen - The Cyber Resilience Act and Open Source: What it Means for Maintainers