Cyber Resilience Act (CRA)

Was ist das und was bedeutet das für KITODO?

CRA – Was ist das?

- Cyber Resilience Act („CRA“) ist eine Regulierung der EU
- Sie enthält Vorschriften für Produkte mit digitalen Elementen („PDE“), um die Cybersicherheit solcher Produkte zu gewährleisten
- „Cybersicherheit“ = Schutz gegen „Cyberbedrohungen“
- Unmittelbar rechtlich verbindlich für alle (ohne, dass die EU-Mitgliedsstaaten das in nationales Recht umsetzen müssen)
- In Kraft getreten → Dez 2024
- Erste verpflichtende Umsetzungen → Sep 2026
- Volle Umsetzung von allen Beteiligten → Dez 2027

Präambel

- Die Cybersicherheit bedeutet eine der größten Herausforderungen für die Union ...
- Cyberangriffe sind ein Thema von öffentlichem Interesse, da sie sich nicht nur auf die Wirtschaft der Union, sondern auch auf die Demokratie sowie die Sicherheit und Gesundheit der Verbraucher kritisch auswirken …
- Dabei sollten zwei große Probleme angegangen werden, die hohe Kosten für die Nutzer und die Gesellschaft verursachen:
  - Ein geringes Maß an Cybersicherheit von Produkten …,
  - sowie ein mangelnder Informationszugang der Nutzer, wodurch sie daran gehindert werden, Produkte mit angemessenen Cybersicherheitsmerkmalen auszuwählen …

Kerninhalt

Von Artikel (1):

- a) Vorschriften für ... Produkte mit digitalen Elementen(PDE), um die Cybersicherheit solcher Produkte zu gewährleisten;
- b) ... Cybersicherheitsanforderungen an die Konzeption, Entwicklung und Herstellung von PDE sowie Pflichten ... hinsichtlich der Cybersicherheit;
- c) ... Cybersicherheitsanforderungen ... zur Behandlung von Schwachstellen ...
- d) Vorschriften für die Marktüberwachung ...

Produktgruppen

Grundsätzlich werden alle PDE betrachtet, die im EU-Markt bereitgestellt werden!

- Wichtige PDE – Klasse 1, z.B.
  - Betriebssysteme, Passwort-Manager, Browser, Router, …
- Wichtige PDE – Klasse 2, z.B.
  - VM-Umgebung, Firewalls, …
- Kritische PDE
  - Smart-Meter, Chip-Karten
- Weitere, extra erwähnt kritische PDE: „High Risk AI Systems“
- Ausgeschlossenen Produkt-Gruppen (da anderweitig schon reguliert), z.B. Luftfahrt
- „Rest“ ist „normal“ ➔ KITODO gehört zu „Rest“

Kategorien von „PDE-Erzeugern“

- „Hersteller“:
  - Im Prinzip, was man sich darunter vorstellt – der normale, kommerzielle Fall.
  - Allerdings ist der Begriff sehr weit definiert, so dass man schnell „Hersteller“ wird.
- „Verwalter von Open Source Software“:
  - Das wurde extra in der Feedback-Schleife nach massivem Gegenwind aus der OpenSource-Community eingeführt
  - „Verwalter quelloffener Software“ ist eine juristische Person …, die … das Ziel hat, die Entwicklung spezifischer PDE, die als freie und quelloffene Software gelten und für kommerzielle Tätigkeiten bestimmt sind, systematisch und nachhaltig zu unterstützen, … (aus Art (3))
- Reine, nicht kommerzielle (private) PDEs fallen nicht unter CRA!

Pflichten (Auszug)

Thema	Hersteller	OpenSource-Verwalter
Cybersicherheitsstrategie	x	x
Entwicklung gemäß „GRUNDLEGENDE CYBERSECURITYANFORDERUNGEN“ (Anhang I, Teil 1)	X	-
Risiko-Mgmt	x	-
Meldepflichten	x	x
Technische Dokumentation	x	-
SBOM	x	-
CE-Konformität	x	- (nicht erlaubt)
Mögliche Sanktionen (Geldstrafe)	x	-

CRA <-> KITODO

- Heute ist das nur ein Einstieg
- Ob bzw. wie KITODO im CRA „mitspielt“ ist zu diskutieren und dann festzulegen
- Weitere Diskussion gerne im Barcamp, z.B.
  - Welche formale Rolle hat KITODO e.V. ? (Hersteller, Verwalter, oder… ?)
  - Was soll inhaltlich von der CRA umgesetzt werden (z.B. SBOM erstellen wir ja sogar schon …) ?
  - ….

Kontakt

CCS Content Conversion Specialists – Hamburg/Germany

Stefan von der Heide (CTO)

Stefan.vonderHeide@content-conversion.com

Telefon: +49 1579 2366592

info@content-conversion.com

www.content-conversion.com

Backup

Begriffe

- „*Cybersicherheit*“ umfasst u.a. Risikomanagement, **Prävention** (Härtung, Zugriffskontrollen, Verschlüsselung), **Erkennung** (Monitoring), **Reaktion** (Incident Handling) und **Wiederherstellung** – mit dem Ziel, Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von IT-Systemen zu wahren. (Zusammengefasst von ChatGPT aus Art. 2 Nr. 1 und Nr. 8 der Verordnung (EU) 2019/881.)
- „PDE“: Ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in den Verkehr gebracht werden (aus der Richtlinie)

Anhang I, Teil 1

ANHANG I

GRUNDLEGENDE CYBERSECURITYANFORDERUNGEN

Teil I Cybersicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen

(1) Produkte mit digitalen Elementen werden so konzipiert, entwickelt und hergestellt, dass sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten.

(2) Auf der Grundlage der Bewertung der Cybersicherheitsrisiken gemäß Artikel 13 Absatz 2 müssen Produkte mit digitalen Elementen, soweit zutreffend,

a) ohne bekannte ausnutzbare Schwachstellen auf dem Markt bereitgestellt werden,

b) mit einer sicheren Standardkonfiguration auf dem Markt bereitgestellt werden, sofern zwischen dem Hersteller und dem gewerblichen Nutzer in Bezug auf ein maßgeschneidertes Produkt mit digitalen Elementen nichts anderes vereinbart wurde, und die Möglichkeit bieten, das Produkt in seinen ursprünglichen Zustand zurückzusetzen,

c) sicherstellen, dass Schwachstellen durch Sicherheitsaktualisierungen behoben werden können, gegebenenfalls auch durch automatische Sicherheitsaktualisierungen, die als Standardeinstellung innerhalb eines angemessenen Zeitrahmens installiert werden sowie über einen klaren und benutzerfreundlichen Opt-out-Mechanismus verfügen, bei dem die Nutzer über verfügbare Aktualisierungen informiert werden und sie vorübergehend verschieben können;

d) durch geeignete Kontrollmechanismen Schutz vor unbefugtem Zugriff bieten, darunter u. a. zumindest Authentifizierungs-, Identitäts- oder Zugangsverwaltungssysteme, und einen möglicherweise unbefugten Zugriff melden,

e) die Vertraulichkeit gespeicherter, übermittelter oder anderweitig verarbeiteter personenbezogener oder sonstiger Daten schützen, z. B. durch Verschlüsselung relevanter Daten, die gespeichert sind oder gerade verwendet oder übermittelt werden, durch modernste Mechanismen und durch den Einsatz anderer technischer Mittel,

f) die Integrität gespeicherter, übermittelter oder anderweitig verarbeiteter Daten, ob personenbezogener oder sonstiger Daten, Befehle, Programme und Konfigurationen vor einer vom Nutzer nicht genehmigten Manipulation oder Veränderung schützen und deren Beschädigung melden,

g) die Verarbeitung personenbezogener oder sonstiger Daten auf solche, die angemessen und von Bedeutung sind, und auf das für die Zweckbestimmung des Produkts mit digitalen Elementen erforderliche Maß beschränken („Datenminimierung"),

h) die Verfügbarkeit wesentlicher und grundlegender Funktionen, auch nach einem Sicherheitsvorfall, einschließlich über Abwehr- und Eindämmungsmaßnahmen gegen Überlastungsangriffe auf Server (Denial-of-Service-Angriffe), sicherstellen,

i) die negativen Auswirkungen von den Produkten selbst oder von vernetzten Geräten auf die Verfügbarkeit der von anderen Geräten oder Netzen bereitgestellten Dienste minimieren,

j) so konzipiert, entwickelt und hergestellt werden, dass sie — auch bei externen Schnittstellen — möglichst geringe Angriffsflächen bieten,

k) so konzipiert, entwickelt und hergestellt werden, dass die Auswirkungen eines Sicherheitsvorfalls durch geeignete Mechanismen und Techniken zur Minderung der möglichen Ausnutzung verringert werden,

l) sicherheitsbezogene Informationen durch Aufzeichnung und/oder Überwachung einschlägiger interner Vorgänge wie Zugang zu Daten, Diensten oder Funktionen und Änderungen daran bereitstellen und den Nutzern einen Opt-out-Mechanismus zur Verfügung stellen,

m) den Nutzern die Möglichkeit bieten, alle Daten und Einstellungen dauerhaft sicher und einfach zu löschen, und, wenn diese Daten auf andere Produkte oder Systeme übertragen werden können, sicherstellen, dass dies auf sichere Weise geschieht.

Links

- EU-Richtlinie: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32024R2847
- Linux-Foundation-Online-Course: https://trainingportal.linuxfoundation.org/courses/understanding-the-eu-cyber-resilience-act-cra-lfel1001
- BSI-Information: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html