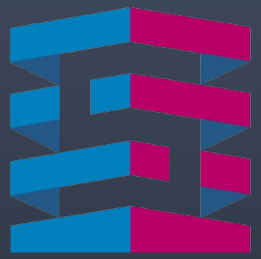


Stackable

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

Bitkom Forum Open Source - 12 September 2024
Lars Francke - https://stackable.tech

Cyber Resilience Act / Disclaimer

Dieser Talk bezieht sich auf die öffentliche Version des CRA vom 18. Juli 2024 (“Corrigendum”)

https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130-FNL-COR01_EN.pdf
https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html

- Theoretisch kann sich daran noch was ändern aber…
- Veröffentlichung wird jetzt für Mitte/Ende November 2024 erwartet
- Ich bin kein Anwalt und das hier ist nicht als Rechtsberatung zu verstehen :)

Stackable

Frage 1: Bin ich betroffen

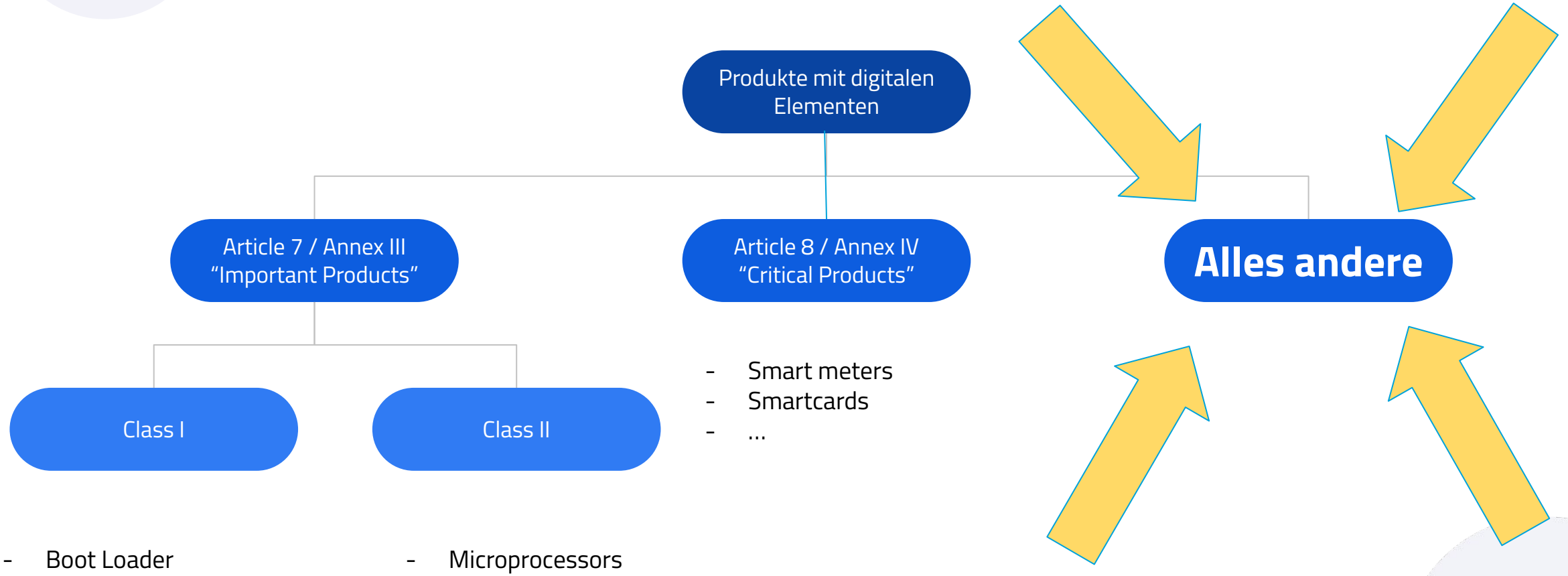
Für diesen Talk: JA!

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

Kurz: “**economic operator**”
(aber nicht “**steward**”)

Stackable

Frage 2: Was bin ich?



- Smart meters
- Smartcards
- ...

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

- Microprocessors
- Container Runtime Systems (Kubernetes) & Hypervisor
- Firewalls, IDS etc
- ....

Stackable

Was müssen wir
- Stackable -
konkret tun?

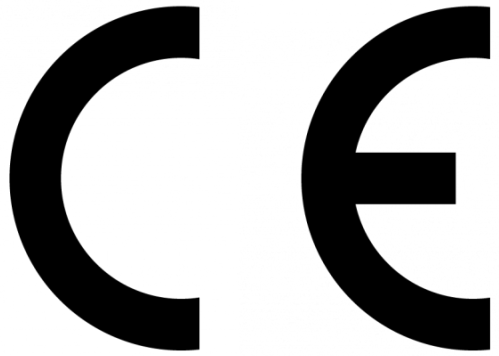
CRA: Schritte zur Konformität

1	CE marking	Artikel 30

Stackable

CE Zeichen / Artikel 30

Kurz gesagt:



CRA:

✅

Stackable

Vielen Dank!

Gibt es Fragen?

CRA: Schritte zur Konformität

1	EU declaration of conformity	Artikel 28/32
2	CE marking	Artikel 30

Stackable

EU declaration of conformity

Article 28

EU declaration of conformity

1. The EU declaration of conformity shall be drawn up by manufacturers in accordance with Article 13(12) and state that the fulfilment of the applicable essential cybersecurity requirements set out in Annex I has been demonstrated.

2. The EU declaration of conformity shall have the model structure set out in Annex V and shall contain the elements specified in the relevant conformity assessment procedures set out in Annex VIII. Such a declaration shall be updated ***as appropriate***. It shall be made available in the languages required by the Member State in which the product with digital elements is placed on the market or made available ***on the market***.

Stackable

EU declaration of conformity

- 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**
- Beschreibung des **Conformity Assessment**

Annex V

EU DECLARATION OF CONFORMITY

The EU declaration of conformity referred to in Article 28, 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 its 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 ***with digital elements*** allowing traceability, ***which*** 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):

Stackable

Conformity Assessment?

Conformity Assessment!

Article 32

Conformity assessment procedures for products with digital elements

1. The manufacturer shall perform a conformity assessment of the product with digital elements and the processes put in place by the manufacturer to determine whether the essential cybersecurity requirements set out in Annex I are met. The manufacturer shall demonstrate conformity with the essential cybersecurity requirements by using ***any*** of the following procedures:

(a) the internal control procedure (based on module A) set out in Annex VIII;

(b) the EU-type examination procedure (based on module B) set out in Annex VIII followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VIII;

(c) a conformity assessment based on full quality assurance (based on module H) set out in Annex VIII***; or***

(d) where available and applicable, a European cybersecurity certification scheme pursuant to Article 27(9).

Stackable

Conformity Assessment

Annex VIII

CONFORMITY ASSESSMENT PROCEDURES

Part I Conformity Assessment procedure based on internal control (based on Module A)

1. Internal control is the conformity assessment procedure whereby the manufacturer fulfils the obligations set out in points 2, 3 and 4 of this Part, and ensures and declares on its sole responsibility that the products with digital elements satisfy all the essential cybersecurity requirements set out in Part I of Annex I and the manufacturer meets the essential cybersecurity requirements set out in Part II of Annex I.

2. The manufacturer shall draw up the technical documentation described in Annex VII.

3. Design, development, production and vulnerability handling of products with digital elements

The manufacturer shall take all measures necessary so that the design, development, production and vulnerability handling processes and their monitoring ensure compliance of the manufactured or developed products with digital elements and of the processes put in place by the manufacturer with the essential cybersecurity requirements set out in Parts I and II of Annex I.

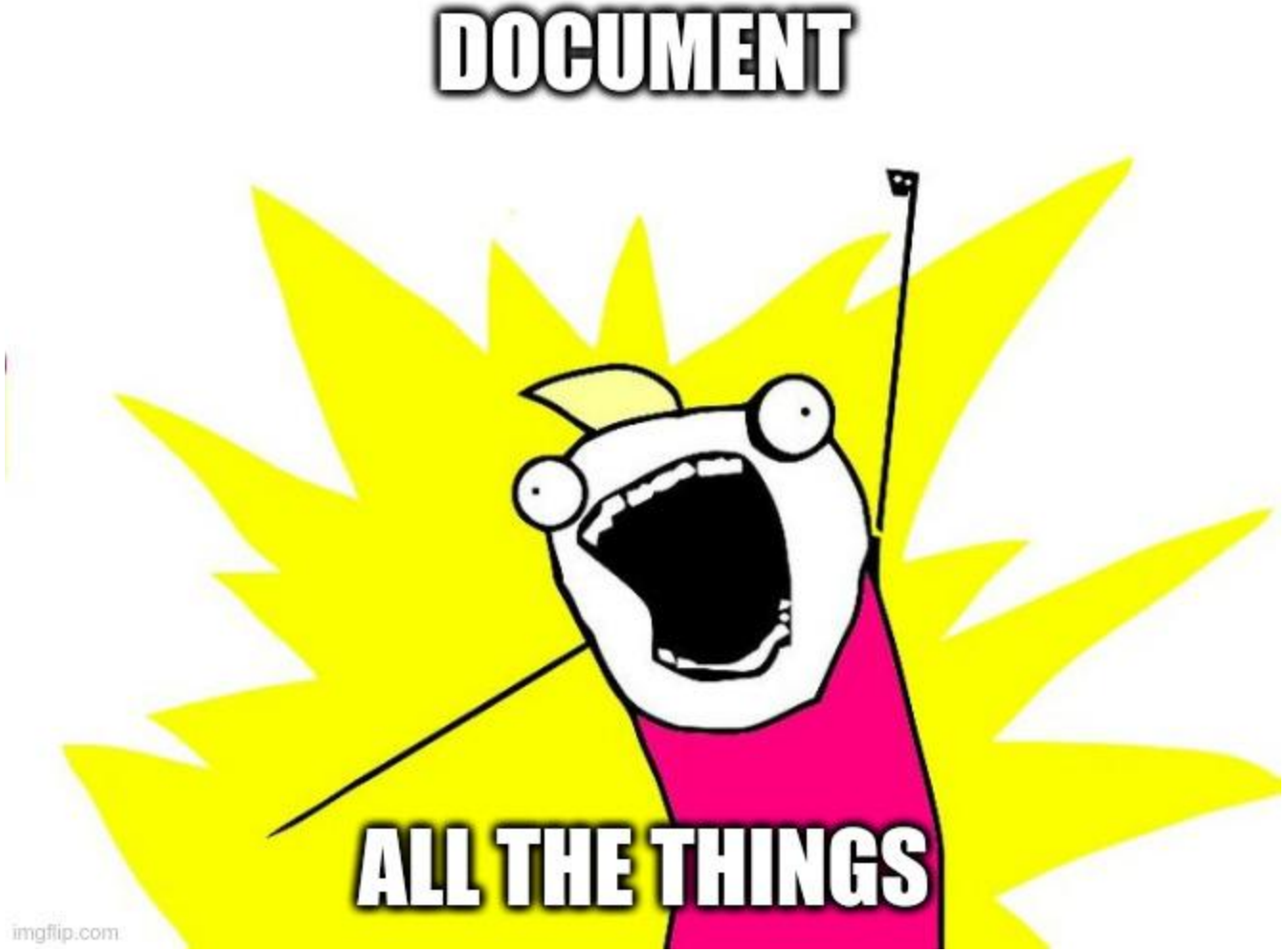
Stackable

CRA: Schritte zur Konformität

1	Dokumentation	Artikel 31
2	EU declaration of conformity	Artikel 28/32
3	CE marking	Artikel 30

Stackable

Dokumentation



Stackable

Dokumentation

Article 31

Technical documentation

1. The technical documentation shall contain all relevant data or details of the means used by the manufacturer to ensure that the product with digital elements and the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Annex I. It shall at least contain the elements set out in Annex VII.

Stackable

Dokumentation / Annex VII

- Produktbeschreibung
- Beschreibung des Software Development Lifecycle (SDLC)
- Vulnerability Management Prozess
- Vulnerability Disclosure Policy
- Supportperiode (und wie man dazu gekommen ist)
- Links zu SBOMs (Software Bill of Materials)
  - Siehe dazu auch BSI TR-03183 Teil 2
  - Kann standardisiert werden
- Beschreibung des Updateverfahrens
- Beschreibung wie alle obigen Prozesse sichergestellt und überwacht werden
- Beschreibung von Tests, die gemacht wurden um CRA “kompatibel” zu sein
- Kopie der *EU declaration of conformity*
- Ergebnis des **Risk Assessment**
- mindestens 10 Jahre aufbewahren

Stackable

Prozesse, Policies und Controls

- Vulnerability Management Prozess
- Vulnerability Disclosure Policy
- Sicherer Software Development Prozess
- Software Lifecycle Policies (EoL, Updates etc.)
- SBOMs

Stackable

CRA: Schritte zur Konformität

1	Risk Assessment	Artikel 13
2	Dokumentation	Artikel 31
3	EU declaration of conformity	Artikel 28/32
4	CE marking	Artikel 30

Stackable

Risk Assessment

CHAPTER II

OBLIGATIONS OF ECONOMIC OPERATORS ***AND PROVISIONS IN RELATION TO FREE AND OPEN-SOURCE SOFTWARE***

Article 13

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 cybersecurity requirements set out in Part I of Annex I.

2. For the purpose of complying with paragraph 1, manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing incidents and minimising their impact, including in relation to the health and safety of users.

Stackable

Risk Assessment

3. *The cybersecurity risk assessment shall be documented and updated as appropriate during a support period to be determined in accordance with paragraph 8 of this Article. That cybersecurity risk assessment shall comprise at least an analysis of cybersecurity risks based on the intended purpose and reasonably foreseeable use, as well as the conditions of use, of the product with digital elements, such as the operational environment or the assets to be protected, taking into account the length of time the product is expected to be in use. The cybersecurity risk assessment shall indicate whether and, if so in what manner, the security requirements set out in Part I, point (2), of Annex I are applicable to the relevant product with digital elements and how those requirements are implemented as informed by the cybersecurity risk assessment. It shall also indicate how the manufacturer is to apply Part I, point (1), of Annex I and the vulnerability handling requirements set out in Part II of Annex I.*

Risk Assessment

- Bewertung der Cybersecurity Risiken eines Produkts nach Annex I Part I
- Ergebnis muss einfließen in Design, Entwicklung, Produktion, Lieferung und Wartung
- Über die Lebensdauer aktuell halten
- Muss Begründung beinhalten falls gewisse Punkte nicht relevant sind
- Die Bewertung muss Teil der technischen Dokumentation sein (Article 31 / Annex VII)

Stackable

CRA: Schritte zur Konformität

1	Cybersecurity Requirements	Annex I
2	Risk Assessment	Artikel 13
3	Dokumentation	Artikel 31
4	EU declaration of conformity	Artikel 28/32
5	CE marking	Artikel 30

Stackable

Annex I, Part I: Essential Cybersecurity Requirements

- Keine bekannten ausnutzbaren Schwachstellen (*known exploitable vulnerabilities*)
- Secure by Default
- 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)
- Verfügbarkeit (Availability) durch Resilienz
- Datenminimalismus (Privacy)
- Audit Funktionalität
- Möglichkeit zum Löschen aller Daten
- ...

Stackable

Stackable

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

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

- Die ganze Prozedur muss (theoretisch) erneut für jede neue Version durchgeführt werden
  - Einbindung in kontinuierlichen Entwicklungsprozess sinnvoller
- Security Updates müssen geliefert werden
- Es reicht die letzte Version zu unterstützen solange Nutzer kostenlosen Zugriff darauf haben und es keine signifikanten zusätzlichen Kosten gibt um darauf zu aktualisieren
- 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

Stackable

Schwachstellenmanagement
Annex I, Part II: Vulnerability Handling Requirements

- SBOMs
- Schwachstellen (Eigene & Third Party)
  - Dokumentieren / Informieren / Public Disclosure
    - Maschinenlesbar / VEX Statements / z.B. CSAF
  - Innerhalb von 24h an ENISA melden (actively exploited, impact on security)
  - Behandeln: z.B. durch kostenlose Updates
- Regelmäßige Tests und Security Reviews
- Policy zu Coordinated Vulnerability Disclosure
- Alle Hardware und Software Fixes, die man entwickelt müssen (kostenlos) mit upstream maintainern geteilt werden

Stackable

CRA

Stackable

Zusammenfassung: Artikel 13 - Obligations of manufacturers

12. Before placing a product with digital elements on the market, manufacturers shall draw up the technical documentation referred to in Article 31.

They shall carry out the chosen conformity assessment procedures as referred to in Article 32 or have them carried out.

Where compliance of the product with digital elements with the essential cybersecurity requirements set out in Part I of Annex I and of the processes put in place by the manufacturer with the essential cybersecurity requirements set out in Part II of Annex I has been demonstrated by that conformity assessment procedure, manufacturers shall draw up the EU declaration of conformity in accordance with Article 28 and affix the CE marking in accordance with Article 30.

Stackable

Zusammenfassung: Artikel 27 - Presumption of conformity

Article 27

Presumption of conformity

Products with digital elements and processes put in place by the manufacturer which are in conformity with harmonised standards or parts thereof, the references of which have been published in the *Official Journal of the European Union*, shall be presumed to be in conformity with the essential cybersecurity requirements ***set out in Annex I*** covered by those standards or parts thereof.

Stackable

Draft standardisation request to European Standards Organisations

ANNEX I

List of new European Standards and/or European standardisation deliverables to drafted

Reference information		Deadline for the adoption by the ESOs
Horizontal standards for security requirements relating to the properties of products with digital elements		
1.	European standard(s) and/or European standardisation deliverable(s) on designing, developing and producing products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on the risks	30/08/2026
2.	European standard(s) and/or European standardisation deliverable(s) on making products with digital elements available on the market without known exploitable vulnerabilities	30/10/2027
3.	European standard(s) and/or European standardisation deliverable(s) on making products with digital elements available on the market with a secure by default configuration	30/10/2027

Horizontale Standards:

- 30 August 2026
- 30 Oktober 2027

Vertikale Standards:

- 30 Oktober 2026

https://ec.europa.eu/docsroom/documents/58974

Stackable

Standards

Horizontal

- Designing, developing and producing secure products
- Vulnerability Management
- Secure by default
- Security updates
- Authentication & Authorization & Auditing & Logging
- Confidentiality & Integrity & Availability
- Data Privacy & Deletion

Vertikal

- Identity Management
- Browsers
- Password Manager
- Malware Protection
- VPN
- Netzwerkinfrastruktur
- Firewall / IDS
- SIEM
- Zertifikats Infrastruktur
- Microprocessors / -controller, FPGAs etc.
- Smart Home Produkte
- Spielzeug
- “Wearables” (Gesundheit)
- Hypervisor / Container Runtimes
- Smart Meter
- Smartcard

https://ec.europa.eu/docsroom/documents/58974

Stackable

CRA: Schritte zur Konformität

1	Cybersecurity Requirements	Annex I
2	Risk Assessment	Artikel 13
3	Dokumentation	Artikel 31
4	EU declaration of conformity	Artikel 28/32
5	CE marking	Artikel 30

Stackable

Endlich...

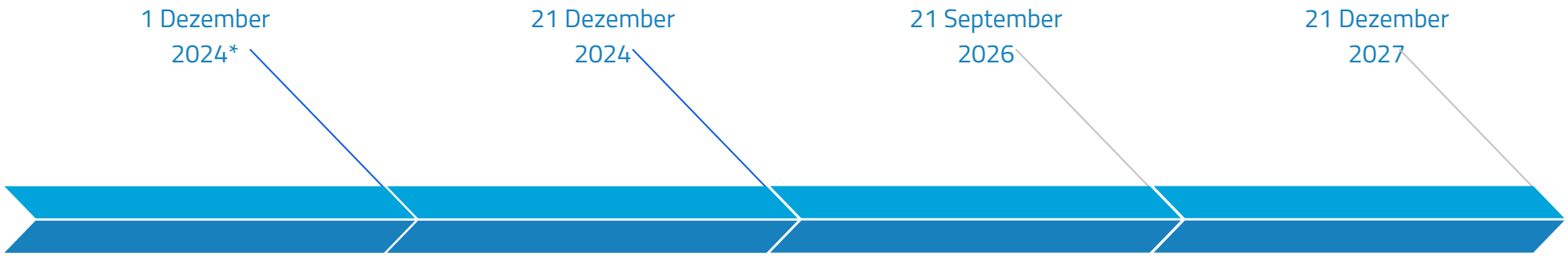
CRA:

✅

Stackable

Timeline - Artikel 71

Horizontale Standards:
- 30 August 2026
- 30 Oktober 2027



Veröffentlichung

Veröffentlichung im Amtsblatt der Europäischen Union

Inkrafttreten

20 Tage nach Veröffentlichung

Meldepflicht für Schwachstellen

21 Monate nach Inkrafttreten müssen aktiv ausgenutzte Schwachstellen und andere schwere Sicherheitslücken gemeldet werden (ENISA)

Endgültiger Start

Die Verordnung gilt 36 Monate nach Inkrafttreten

Stackable

Alle Daten hängen von der tatsächlichen Veröffentlichung ab!

Vielen Dank

Kontakt

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

Stackable