Cyberresiliente Produkte unter dem CRA –
Die wichtigsten Vorgaben für Hersteller

Richard Skalt, Advocacy Manager, Cybersecurity Office (CSO), TÜV SÜD

Freitag, 09.05.2025, 11:00–12:00 Uhr

Add value.
Inspire trust.

Inhalte der heutigen Präsentation

Der Cyber Resilience Act im Überblick

Der Cyber Resilience Act im Überblick

Was ist der Cyber Resilience Act?

- Der Cyber Resilience Act ist die erste EU-weite Regelung, die **verpflichtende Cybersicherheitsanforderungen** an Produkte mit digitalen Elementen über deren **gesamten Lebenszyklus** einführt.
- Der CRA gilt für **alle Produkte mit digitalen Elementen**, die auf dem europäischen Binnenmarkt bereitgestellt werden und mit einem Gerät oder Netzwerk verbunden werden können – einschließlich ihrer Bausteine (z. B. **Hardware und Software**) sowie ihrer **Remote-Datenverarbeitungslösungen**.

Was ist der aktuelle Umsetzungsstand?

- Der Cyber Resilience Act trat am **10. Dezember 2024** in Kraft.
- Die Verpflichtungen zur Meldung von Schwachstellen gelten ab dem **11. September 2026**.
- Die wichtigsten durch die CRA eingeführten Verpflichtungen gelten ab dem **11. Dezember 2027**.

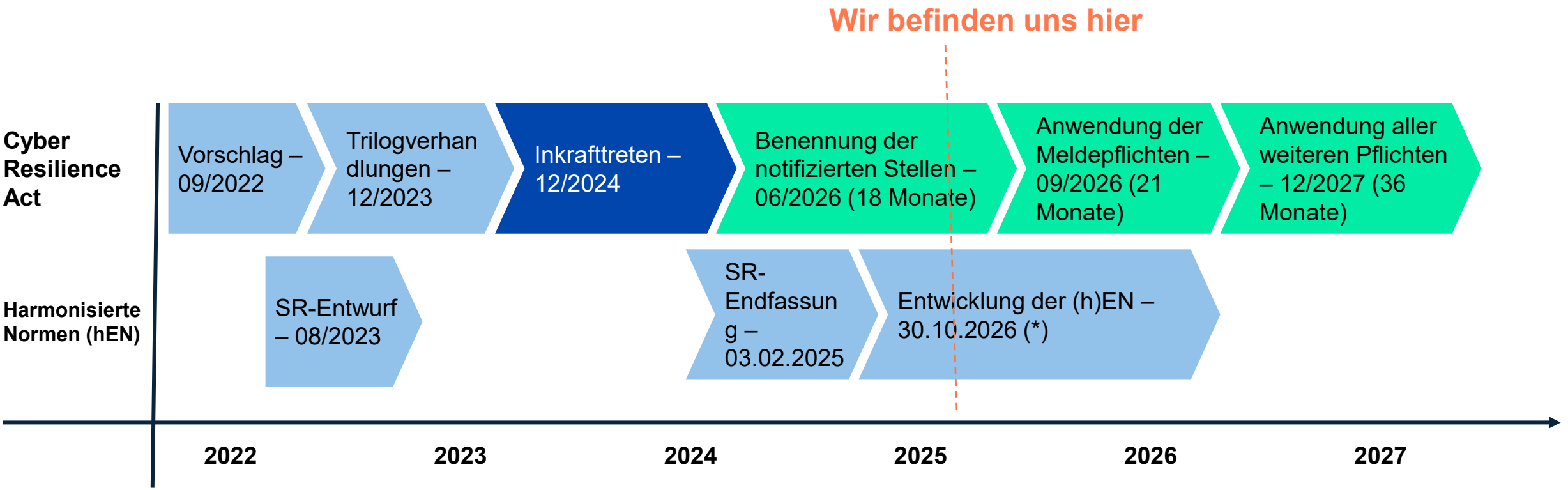
Wer ist betroffen?

- **Hersteller**, **Entwickler**, **Importeure** und **Händler** von Produkten mit digitalen Elementen innerhalb der EU, einschließlich Hardware, Software und IoT-Geräte.
- Gilt für **alle Software- und Hardwareprodukte** sowie für Datenfernverarbeitungslösungen, mit der Ausnahme speziell regulierter Produkte (z. B. Cloud-Angebote – hier gilt NIS-2)

Welche Anforderungen umfasst er?

- Produkte müssen **mit Blick auf Cybersicherheit entworfen und entwickelt** werden („Security by Design“), um bekannte Schwachstellen zu mindern und potenzielle Risiken zu managen.
- **Umgang mit Schwachstellen** über den gesamten Produktlebenszyklus hinweg (für den Zeitraum, in dem das Produkt voraussichtlich verwendet wird).
- **Produktbezogene Cybersicherheits-Risikoanalysen** und (abhängig von der Produktkategorie) verpflichtende **Konformitätsbewertung**.
- **Meldepflichten** für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle, die die Produktsicherheit betreffen.

Zeitstrahl für die CRA-Umsetzung



Neuentwicklung von 41 harmonisierten Normen (hEN)
- 15 hENs sind produktunabhängige Normen, z. B. zum Entwicklungsprozess oder zum Umgang mit Schwachstellen
- 26 hENs für Produktkategorien

(*) Von der EU angefordertes Datum; für einige Normen früher

Wichtige Meilensteine:
03/2024: EU-Parlament hat abgestimmt und zugestimmt
07/2024: Berichtigung
10/2024: Annahme durch den Rat
20.11.2024: Veröffentlichung im Amtsblatt der EU (2024/2847)

Relevante Regulierungen mit Bezug zum CRA

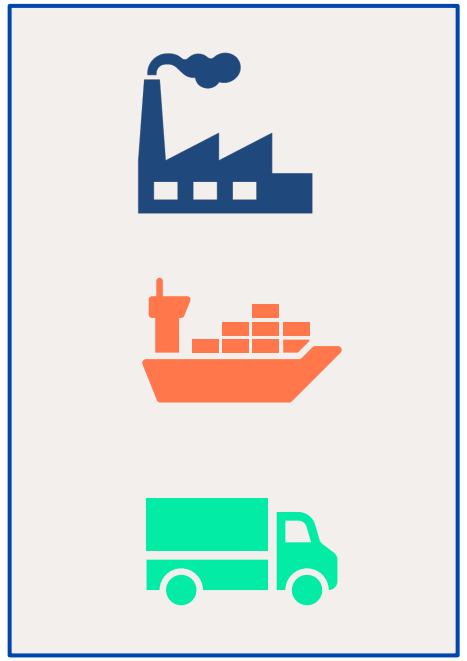
	Cyber Resilience Act	RED DA	NIS2	Machinery Regulation	AI Act
Anforderungen	Cybersicherheitsanforderungen für Hardware- und Softwareprodukte mit digitalen Elementen.	Cybersicherheitsanforderungen für Funkgeräte.	Maßnahmen zum Cybersicherheits-Risikomanagement und Meldepflichten für Organisationen.	Sicherheits- und Cybersicherheitsanforderungen für Maschinen und verwandte Produkte.	Cybersicherheitsaspekte von Künstlicher Intelligenz mit Fokus auf Hochrisiko-KI-Systeme.
Betroffene Akteure	Hersteller, Händler und Importeure von Produkten mit digitalen Elementen in der EU.	Hersteller vernetzter Geräte wie Smartphones, IoT-Geräte und WLAN-Router.	Betreiber wichtiger und wesentlicher Dienste in der EU.	Hersteller, Importeure und Händler von Maschinen in der EU.	KI-Entwickler, -Anbieter und -Anwender in der EU.
Fristen für die Einhaltung	Meldepflichten: **11. September 2026** Vollständig anwendbar: **11. Dezember 2027**	Vollständig anwendbar: **1. August 2025**	Vollständig anwendbar: **17. Oktober 2024** (abhängig von nationaler Umsetzung)	Vollständig anwendbar: **20. Januar 2027**	Anforderungen an KI-Kompetenz & Verbot nicht akzeptabler KI-Systeme: **2. Februar 2025** Vollständig anwendbar: **2. August 2026**
Bezug zur CRA	Beide Regelungen verlangen „Security by Design“ für drahtlose Geräte. RED DA gilt jedoch nur für Funkgeräte, während die CRA für alle vernetzten Geräte gilt.	Beide Regelungen setzen Cybersicherheitsanforderungen für kritische Infrastrukturen und Meldepflichten durch. NIS2 konzentriert sich stärker auf organisatorische Cyberresilienz statt auf Produktsicherheit.	Beide Regelungen stellen ähnliche Anforderungen an Software-Integrität und Updates. Die Maschinenverordnung betrachtet Cybersicherheit aus der Perspektive der Maschinensicherheit, während die CRA breiter gefasst ist.	Beide Regelungen verlangen Cybersicherheit oder Robustheit für Produkte mit KI. Der AI Act regelt KI aus ganzheitlicher Perspektive, während die CRA für alle digitalen Produkte gilt.	

Geltungsbereich des CRA

Geltungsbereich des CRA

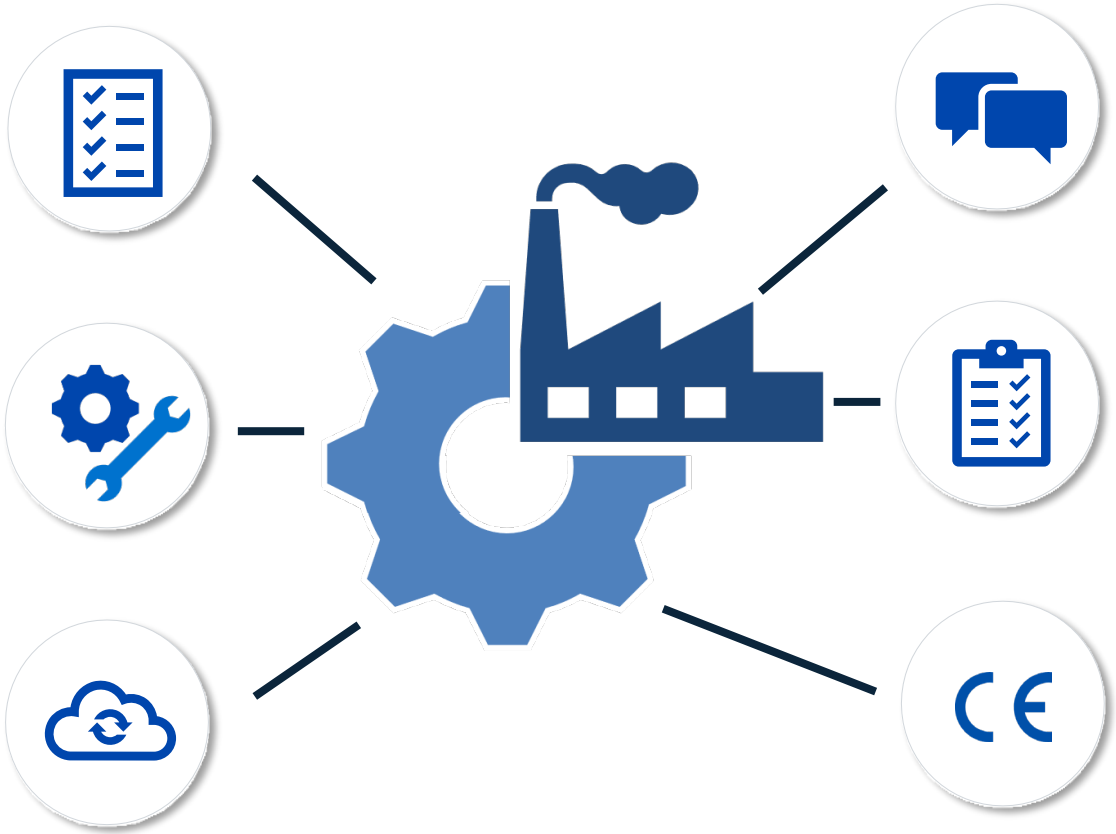
Geltungsbereich nach Wirtschaftsakteuren:

- Relevanz für verschiedene „Wirtschaftsakteure“ (Art. 3 Nr. 12 CRA), insbesondere:
  - **Hersteller**, Pflichten nach Art. 13 ff. CRA; Inverkehrbringen der Produkte
  - **Bevollmächtigte der Hersteller**, Art. 18 CRA; nicht alle Pflichten übertragbar
  - **Importeure**, Pflichten nach Art. 19 CRA; Einführen der Produkte
  - **Händler**, Pflichten nach Art. 20 CRA; Bereitstellen der Produkte auf dem Markt
  - **Quasi-Hersteller**, Art. 22 CRA; jeden, der Änderungen am Produkt vornimmt, treffen die Pflichten des Herstellers bei „**wesentlicher Produktänderung**“
- **OSS-Stewards** (Art. 3 Nr. 14 CRA), Pflichten nach Art. 24 CRA; Entwicklung und Dokumentation von Cybersicherheitsstrategien



CRA-Pflichten für Hersteller

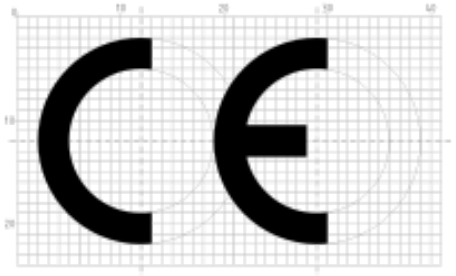
Hersteller müssen die Cybersicherheit über den gesamten Produktlebenszyklus hinweg sicherstellen, was mit umfangreichen Pflichten verbunden ist:

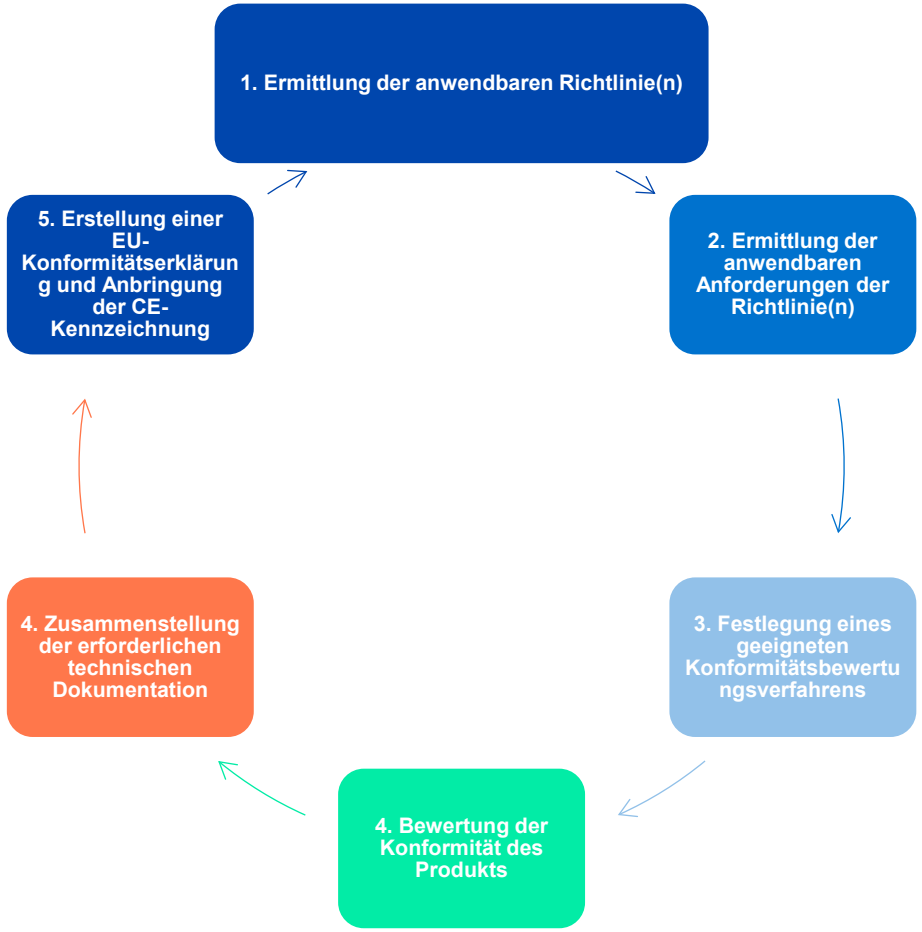


- Produkt-Risikobewertung
- Schwachstellen-management
- Sicherheitsupdates
- Meldepflichten
- Benutzeranleitungen
- Konformitätsbewertung (CE-Kennzeichnung)

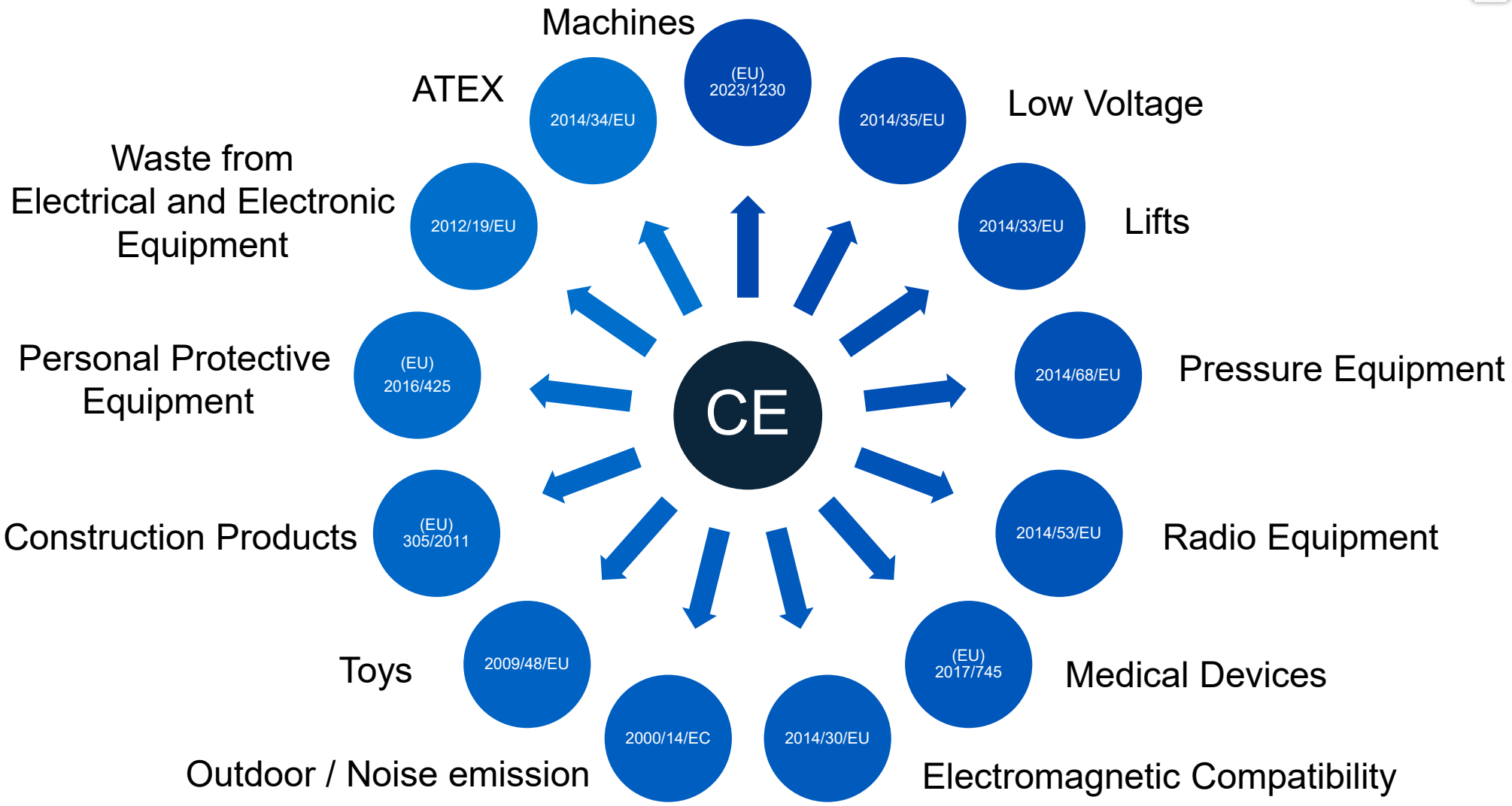
CE-Kennzeichnung für Hersteller

- Die **CE-Kennzeichnung** zeigt an, dass Produkte, die innerhalb des europäischen Binnenmarkts verkauft werden, den Anforderungen an **Gesundheit, Sicherheit und Umweltschutz** entsprechen.
- Die CE-Kennzeichnung ist die **Herstellererklärung**, dass das Produkt den Spezifikationen entspricht.
- Die CE-Kennzeichnung ist für bestimmte Produktgruppen, die im europäischen Binnenmarkt verkauft werden sollen, **verpflichtend**.
- Die Anforderungen werden durch **Produktsicherheitsrichtlinien** geregelt.





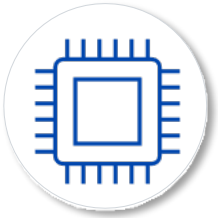
European CE Directives



… and many more Product Directives

Produkte im Geltungsbereich des CRA

Produkte im Geltungsbereich



Hardware Produkte (einschließlich auf den Markt gebrachter Komponenten)
(Laptops, intelligente Geräte, Mobiltelefone, Netzwerkausrüstung oder CPUs…)

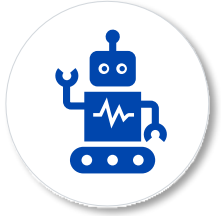
Softwareprodukte (einschließlich auf den Markt gebrachter Komponenten)
(Betriebssysteme, Textverarbeitungsprogramme, Spiele oder mobile Apps, Softwarebibliotheken…)

+

…einschließlich ihrem **Datenfernverarbeitungslösungen**!

Produkte außerhalb des Geltungsbereichs

Dienste (einschließlich eigenständiger SaaS, die unter NIS2 fallen)
(Websites, webbasierte Angebote …)



Nicht-kommerzielle Produkte
(Hobbyprodukte)

Produkte, die unter andere Vorschriften fallen (z. B. EU-MDR, UNECE R 155 …)
(Autos, Medizinprodukte, In-vitro-Diagnostika, zertifizierte Luftfahrtgeräte, Schiffsausrüstung)

Produktklassifizierung & Prüfverfahren

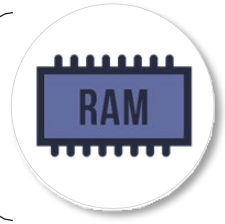
- Einstufung in einfache, wichtige (Klasse I/II) und kritische Produkte
- Der CRA ordnet Produkte in **4 Sicherheitskategorien** ein:
  - (einfache) Produkte mit digitalen Elementen
  - wichtige Produkte mit digitalen Elementen (Klasse I)
  - wichtige Produkte mit digitalen Elementen (Klasse II)
  - kritische Produkte mit digitalen Elementen
- Nach Art. 32 CRA muss **für jedes Produkt eine Bewertung durchgeführt werden, ob die grundlegenden Anforderungen des Anhangs I eingehalten werden**
- Bewertung erfolgt **durch Hersteller selbst**, anhand von „harmonisierten Normen“ oder durch **unabhängige Dritte**, abhängig von der Kategorie
- **CE-Kennzeichnung** + ggf. **EU-Cybersicherheitszertifikat** (gemäß **EUCC-Schema**)

Produktklassifizierung & Prüfverfahren

Produktkategorien

Konformitätsprüfung

90 % der Produkte (nicht kritisch)



Standardkategorie (Art. 2 Abs. 1)
(Speicherchips, mobile Apps, intelligente Lautsprecher, Computerspiele...)

→ **Selbsteinschätzung (Self assessment)**

10 % der Produkte (wichtig und kritisch)

Wichtige Produkte – Klasse I & Klasse II (Art. 7 und Anhang III)
(Klasse I: Betriebssysteme, Antivirenprogramme, Router…
Klasse II: Firewalls, Intrusion-Detection-Systeme)

→ Für **Produkte der Klasse I**: **Anwendung harmonisierter Normen** oder **unabhängige Prüfung**

→ Für **Produkte der Klasse II**: **unabhängige Prüfung**, basierend auf:

- **Funktionalität** (z. B. kritische Software)
- **Verwendungszweck** (z. B. industrielle Steuerung/NIS2)
- **Weitere Kriterien** (z. B. Ausmaß der Auswirkungen)

Kritische Produkte (Art. 8 und Anhang IV)
(Smartcards, Secure Elements, Smart-Meter-Gateways…)

→ **Konformitätsbewertung für kritische Produkte:**
Certification according to the EUCC scheme

Nichtkommerzielle Produkte (nicht betroffen)

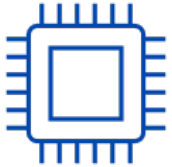
Free and Open Software (FOSS)
(Webentwicklungs-Frameworks, Betriebssysteme, Datenbankmanagementsysteme…)

→ **Selbsteinschätzung (Self assessment)**

Sicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen

Produkte mit digitalen Elementen

… müssen so entworfen, entwickelt und hergestellt werden, dass eine angemessene Cybersicherheit gewährleistet ist, basierend auf der Risikobewertung zur Cybersicherheit.



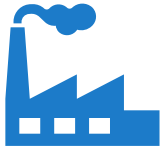
Bereitstellung ohne ausnutzbare Schwachstellen	Secure by Default Konfiguration	Software Updates	Access Control

Vertraulichkeit und Integrität der Daten	Security Logging	Verfügbarkeit wesentlicher Funktionen	Steuerung des Daten-abflusses

Datenlöschung	Begrenzung von Angriffsflächen	Begrenzung der Auswirkungen von Angriffen	Minimierung der Daten-verarbeitung

Product Lifecycle Management

Um Cybersicherheit über den **gesamten Produktlebenszyklus** hinweg aufrechtzuerhalten, muss ein Hersteller das Prinzip **„Security by Default“** anwenden und das Produkt so lange unterstützen, wie es in Gebrauch ist.



Design, Entwicklung & Produktion | **Marktplatzierung** | **Fortlaufende Unterstützung**

- Produkte sollen gemäß dem Prinzip **Security by Default** entworfen, entwickelt und produziert werden.
- Produkte benötigen die **CE-Kennzeichnung**.

- Produkte müssen im Betrieb für sich selbst und andere sicher bleiben.
- **Sicherheitsupdates** müssen für **mindestens 5 Jahre** bereitgestellt werden (gerechnet für jedes individuelle Produkt).

CRA-Anforderungen an Entwicklung und After-Sales-Services

- Hersteller müssen die **Cybersicherheitsrisiken und Anforderungen eines Produkts** in allen Phasen der Produktentwicklung detailliert bewerten.
- Hersteller müssen **regelmäßige Audits/Tests und Bewertungen durchführen**, um die Sicherheit der Produkte während der Supportphase zu überprüfen.
- Es muss darauf geachtet werden, dass **Dritte** (z. B. Lieferanten) und **Open-Source-Komponenten** die **Produktsicherheit nicht beeinträchtigen**.
- Um Produktkomponenten und Schwachstellen zu verfolgen, verlangt die CRA von den Herstellern die **Erstellung einer Software-Stückliste** (SBOM).

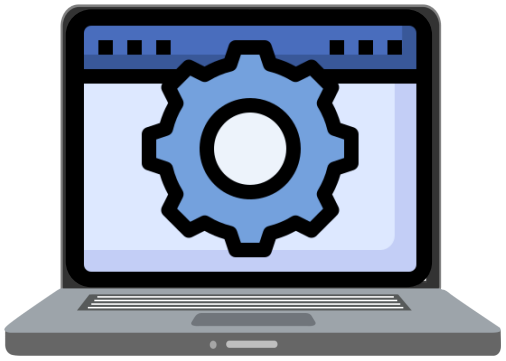
CRA-Anforderungen für Schwachstellenmanagement

- Anbieter benötigen Prozesse zum **Schwachstellenmanagement**.
- Anbieter benötigen eine Organisation/Plattform zur **Meldung von Schwachstellen** an:
  - **Zentrale EU-Meldestelle** (ENISA)
  - **Kunden** (Koordinierte Offenlegung von Schwachstellen)
- Je nach Möglichkeit, können automatisierte Sicherheitsupdates und Informationen diese Vorgaben erfüllen.
- Sofern technisch möglich, sollten Sicherheitsupdates von funktionalen Updates getrennt werden.

- **ENISA** (in Zusammenarbeit mit dem **CSIRTs-Netzwerk** der EU) wurde mit Aufbau, Wartung und sicherem Betrieb einer **einheitlichen Meldeplattform** ab dem **11. September 2026** beauftragt.

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

CSIRTs NETWORK



Zentrale Meldeplattform

CRA-Anforderungen zur Meldung von Schwachstellen

- **Meldung sicherheitsrelevanter Schwachstellen (Vorfälle)** an die zentrale EU-Meldestelle.
- Innerhalb von **max. 24 Stunden** muss die Schwachstelle gemeldet werden.
- Innerhalb von **max. 72 Stunden** muss eine **umfassende Beschreibung** des Vorfalls erfolgen.
- Im Fall eines **Hacks** (Ausnutzung der Schwachstelle) müssen **innerhalb von max. 14 Tagen** Maßnahmen zur Schadensbegrenzung und ein Abschlussbericht eingereicht werden.

Aktiv ausgenutzte Schwachstelle

Der Hersteller muss eine aktiv ausgenutzte Schwachstelle, sobald er davon erfährt, gleichzeitig an das CSIRT und an ENISA melden.

< 24 Std.	< 72 Std.	< Patch + 14 Tage
Frühe Warnung	Schwachstellenmeldung	*Abschlussbericht*

Schwerwiegende Sicherheitsvorfälle

Der Hersteller muss innerhalb von 24 Std. jede schwerwiegende Auswirkung auf die Sicherheit des Produkts melden.

< 24 Std.	< 72 Std.	< 1 Monat
Frühwarnung	Vorfallmeldung	Abschlussbericht

Benachrichtigung der Nutzer

Sobald eine aktiv ausgenutzte Schwachstelle oder ein schwerwiegender Vorfall bekannt wird, muss der Hersteller betroffene Nutzer – und wo angebracht alle Nutzer – zeitnah informieren.

< zeitnah
CSIRT können Nutzer informieren

Anforderungen zum Umgang mit Schwachstellen

Abhängigkeiten und Schwachstellen identifizieren und dokumentieren, einschließlich SBOM (Softwarestückliste).

Sicherheit des digitalen Produkts testen.

Eine koordinierte Richtlinie zur Schwachstellenoffenlegung einführen.

Mechanismen für sicheres Aktualisieren bereitstellen und Sicherheitsupdates liefern.

Keine bekannten Schwachstellen unbeantwortet lassen und existierende unverzüglich beheben.

Informationen über behobene Schwachstellen öffentlich machen.

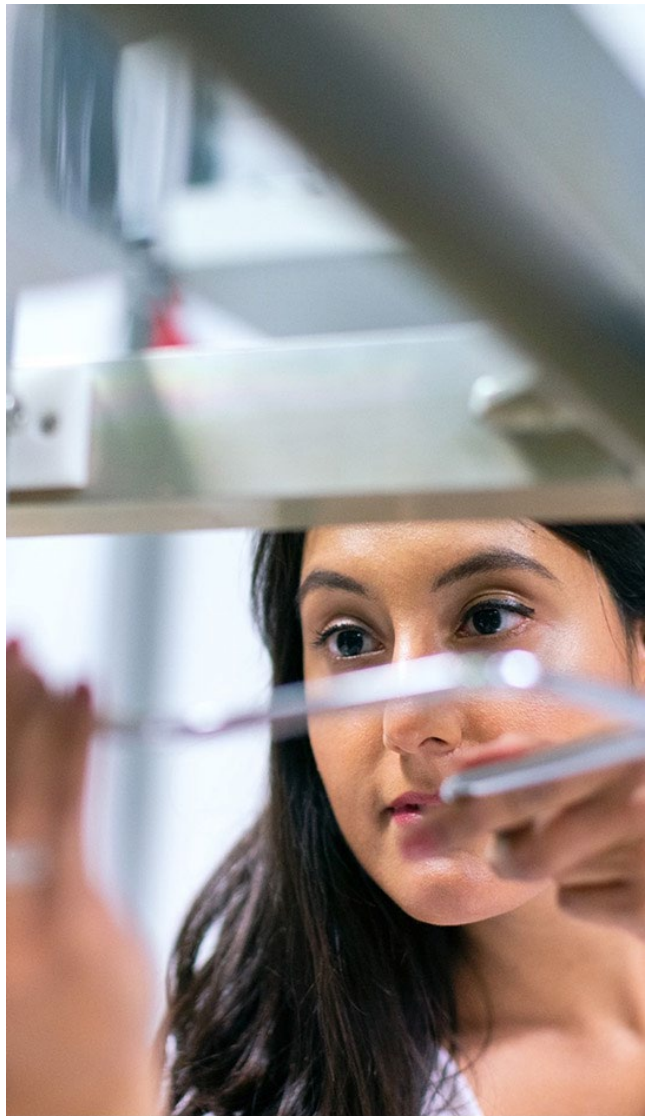
Informationsaustausch über potenzielle Schwachstellen erleichtern.

Patches zeitnah, kostenlos und mit Hinweisen bereitstellen.

CRA-Anforderungen an die Dokumentation

Im Rahmen der CRA müssen Hersteller, Importeure und Händler von Produkten mit digitalen Elementen sicherstellen, dass folgende Informationen verfügbar sind:

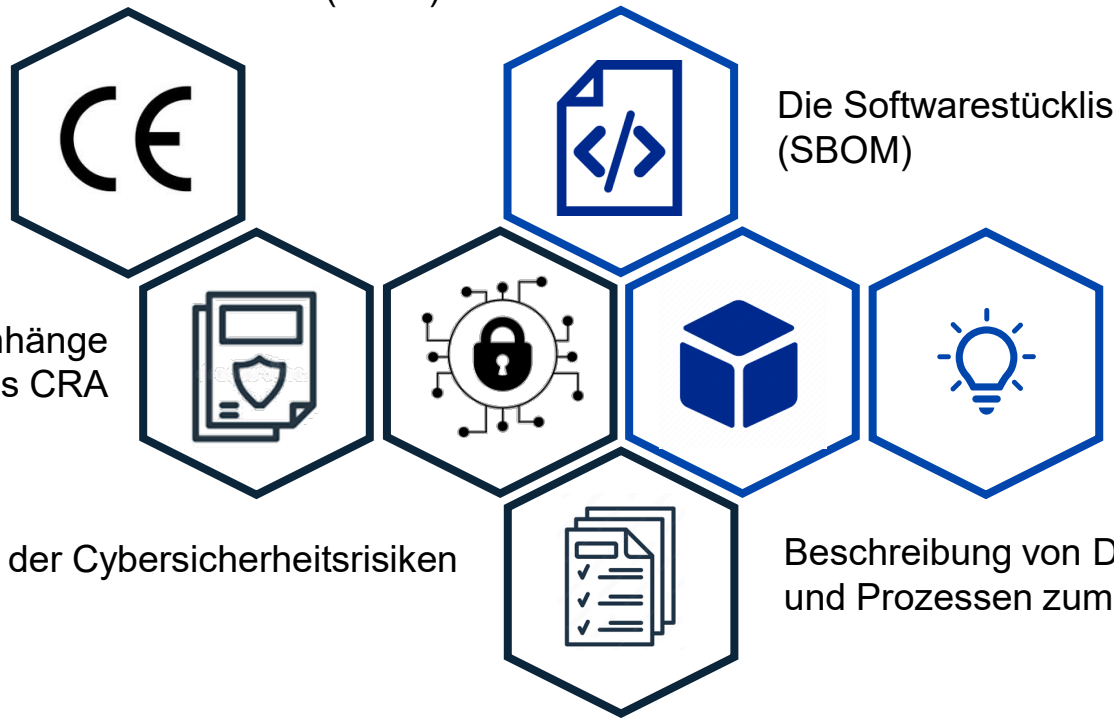
- **Detaillierte Dokumentation** zur **Herstellung** des Produkts
- Ein **zentraler Ansprechpartner** für den Umgang mit Schwachstellen
- **Anleitungen zur Installation von Sicherheitsupdates**
- Anleitungen zur **Aktivierung/Deaktivierung automatischer Sicherheitsupdates**
- Angaben zum **vorgesehenen Verwendungszweck** des Produkts und Informationen zu seinen Sicherheitseigenschaften
- Angaben zu den **bekannten Szenarien und Umständen**, die das Produkt Cybersicherheitsrisiken aussetzen könnten
- **Dauer des Supportzeitraums**
- Anleitung zur **sicheren Inbetriebnahme und Nutzung** des Produkts
- Eine Kopie der **EU-Konformitätserklärung**
- Angabe einer **Softwarestückliste (SBOM)**



Inhalte der Technischen Dokumentation

Angewendete harmonisierte Normen (hENs)

Eine Kopie der EU-Konformitätserklärung



Die Softwarestückliste (SBOM)

Testberichte für die Anhänge I-1 und I-2 des CRA

Allgemeine Beschreibung des Produkts mit digitalen Elementen

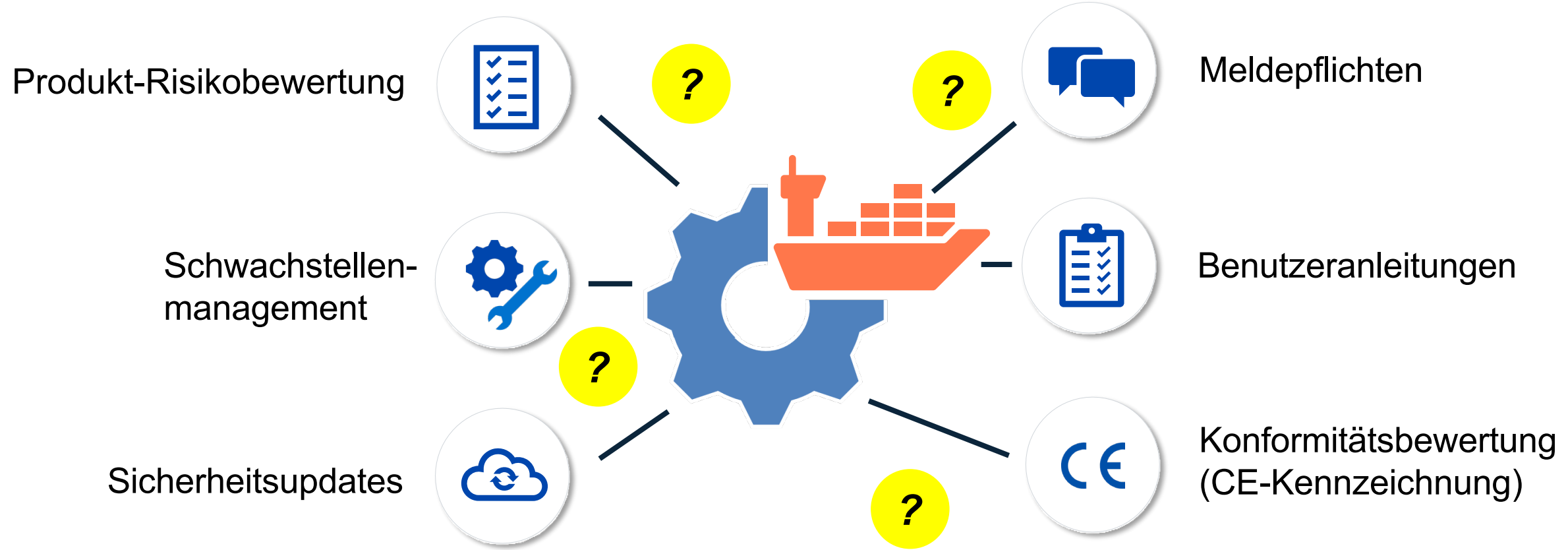
Bewertung der Cybersicherheitsrisiken

Beschreibung von Design, Entwicklung, Produktion und Prozessen zum Umgang mit Schwachstellen

Wie der Supportzeitraum ermittelt wurde

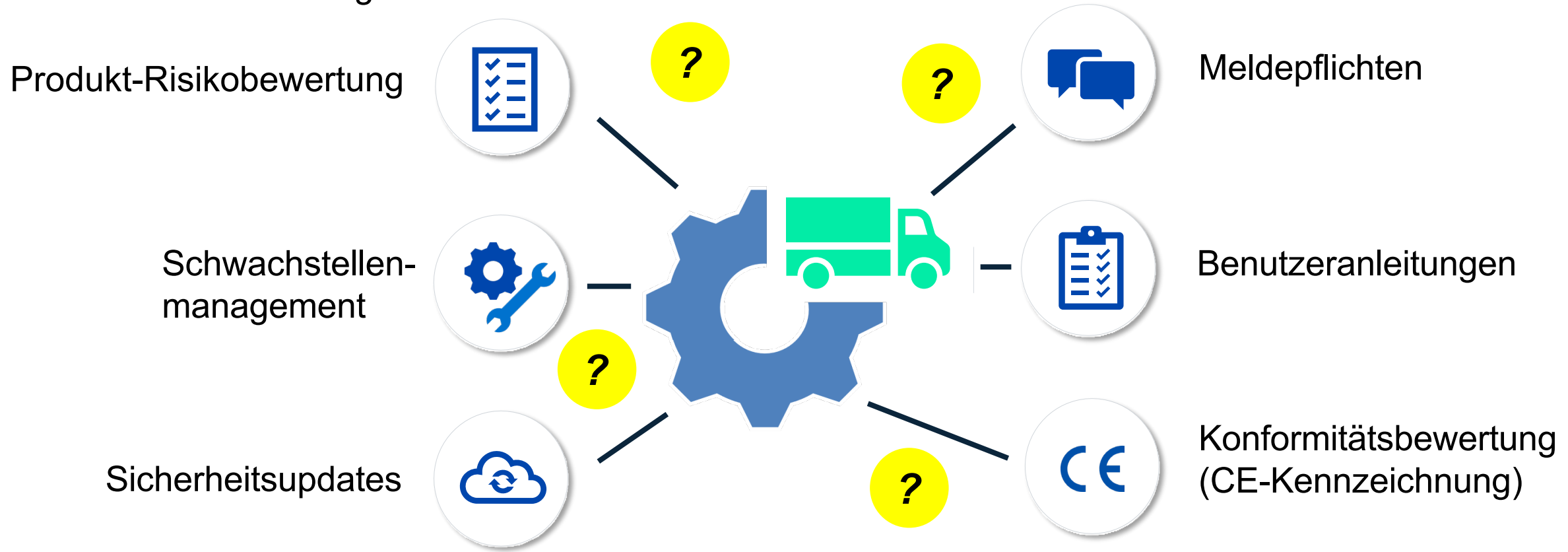
CRA-Pflichten für Importeure

Importeure dürfen **nur Produkte mit digitalen Elementen auf dem Markt bereitstellen, die die Anforderungen an Sicherheit und Schwachstellenmanagement erfüllen**. Es ist ihre Pflicht, die Einhaltung sicherzustellen und bei Abweichungen Korrekturmaßnahmen zu ergreifen.



CRA-Pflichten für Händler

Händler dürfen ebenfalls **nur Produkte mit digitalen Elementen bereitstellen, nachdem sie überprüft haben, dass diese die CE-Kennzeichnung tragen und die Anforderungen an Sicherheit und Schwachstellenmanagement erfüllen**. Bei Nichterfüllung müssen Korrekturmaßnahmen getroffen werden.



Produktanpassung und -änderungen

„wesentliche Änderungen“

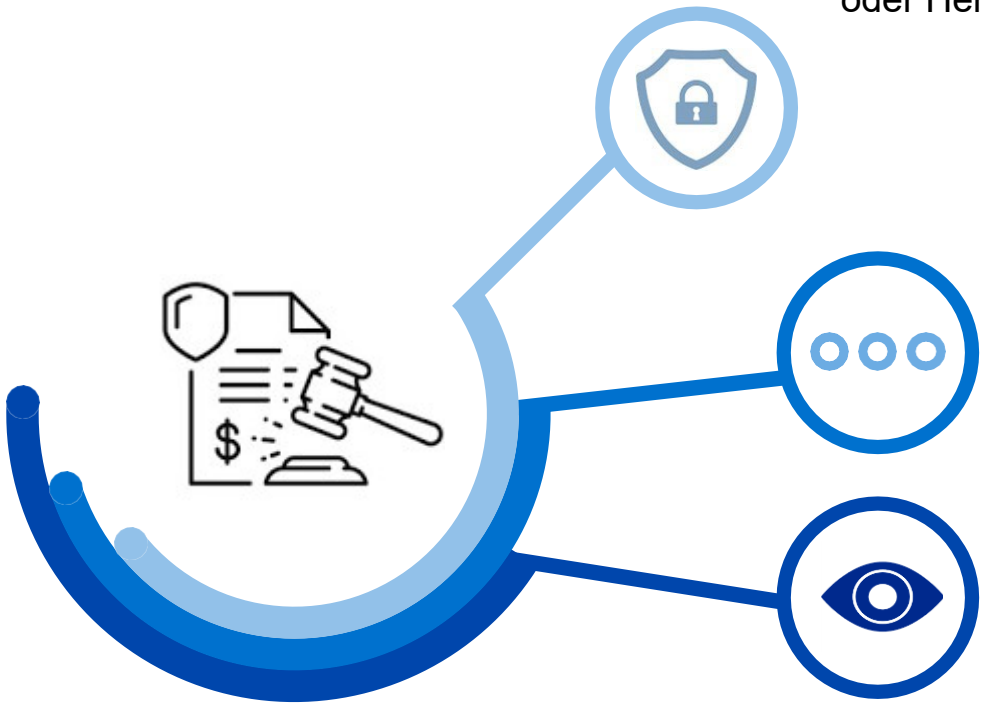
Bezeichnet eine Änderung an einem Produkt mit digitalen Elementen **nach dessen Inverkehrbringen**, **die die Konformität des Produkts mit den wesentlichen Anforderungen gemäß Abschnitt 1 von Anhang I beeinträchtigt** oder zu einer **Änderung des vorgesehenen Verwendungszwecks** führt, für den das Produkt mit digitalen Elementen bewertet wurde;

Wenn ein Importeur oder Händler ein Produkt mit digitalen Elementen unter seinem Namen oder seiner Marke auf den Markt bringt oder eine wesentliche Änderung eines bereits in Verkehr gebrachten Produkts mit digitalen Elementen vornimmt,
→ gilt der Importeur oder Händler als Hersteller.

Weitere Fälle, in denen Herstellerpflichten gelten:

Eine natürliche oder juristische Person, die weder Hersteller, Importeur noch Händler ist, **aber eine wesentliche Änderung an einem Produkt mit digitalen Elementen vornimmt, gilt ebenfalls als Hersteller im Sinne dieser Verordnung**.

Geldstrafen und Sanktionen bei Nichteinhaltung



Bis zu 15.000.000 EUR oder bis zu 2,5 % des weltweiten Jahresumsatzes

Bei Verstoß gegen **grundlegende Cybersicherheitsanforderungen** (Anhang I) oder Herstellerpflichten (Artikel 13, 14)

Bis zu 10.000.000 EUR oder bis zu 2 % des weltweiten Jahresumsatzes

Bei Verstoß gegen Artikel 18–23, 28, 30(1)–(4), 31(1)–(4), 32(1)–(3), 33(5), 39, 41, 47, 49, 53

Bis zu 5.000.000 EUR oder bis zu 1 % des weltweiten Jahresumsatzes

Bei Übermittlung **falscher, unvollständiger oder irreführender Informationen** an benannte Stellen oder Marktüberwachungsbehörden

TÜV SÜD Services

The CRA Compliance Check

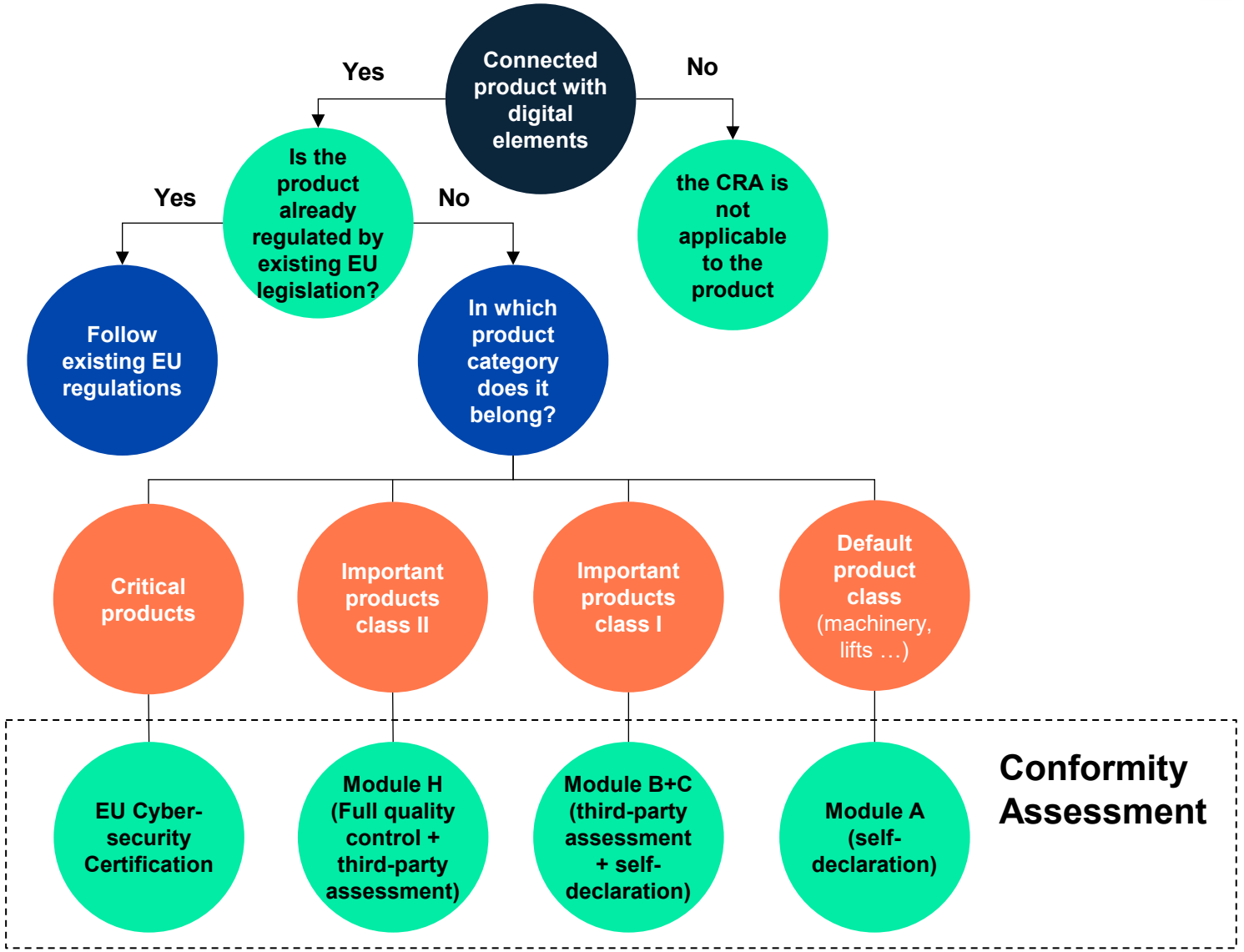
In our **CRA Compliance Check** we can determine

- whether your product falls under the CRA
- which product category it belongs to
- what type of conformity assessment is necessary to comply with the CRA

In case a product is found to be non-conforming, **the product will be forcibly withdrawn from the EU market** and product recall is possible.

Conformity assessment

- The test standard is still being developed within CEN/CENELEC JTC 13.
  - The first draft of the test catalogue is expected End of 2025
- For third-party tests, **CE test labs** are required. ENISA manages a public list of all accredited test labs in EU member states.



Road to CRA compliance – CE marking

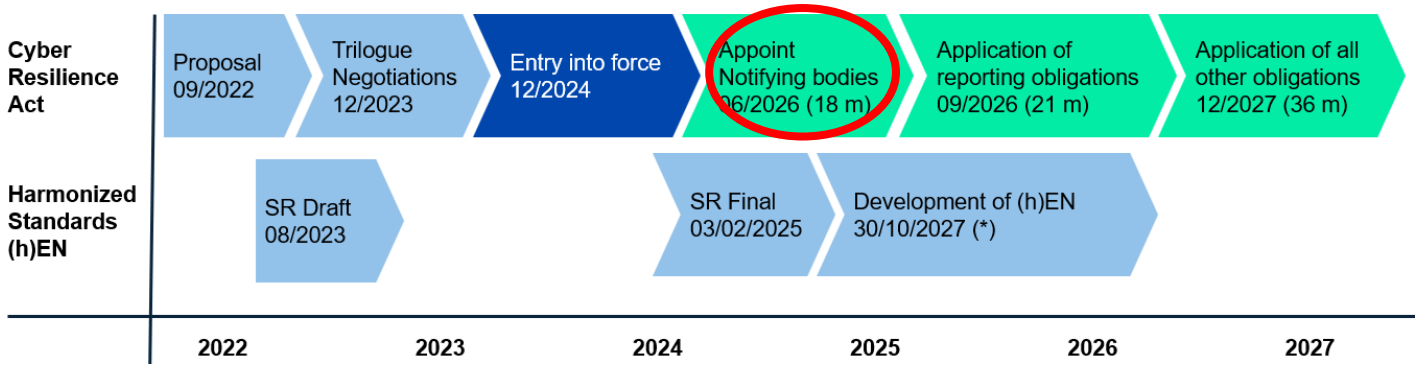
In **June 2026** the notifying Bodies will be appointed.

TÜV SÜD plans to apply to become a notified body in June 2026.

Earliest June 2026 TÜV SÜD can officially confirm product conformity to the CRA and grant you the CE mark

For this TÜV SÜD already started to develop a test-scheme covering the following areas

- Scope applicability
- Cybersecurity Risk assessment
- Vulnerability Handling
- Information to user
- SBOM
- Supply chain due diligence
- Reporting obligations
- Product Security Requirements
- Technical documentation

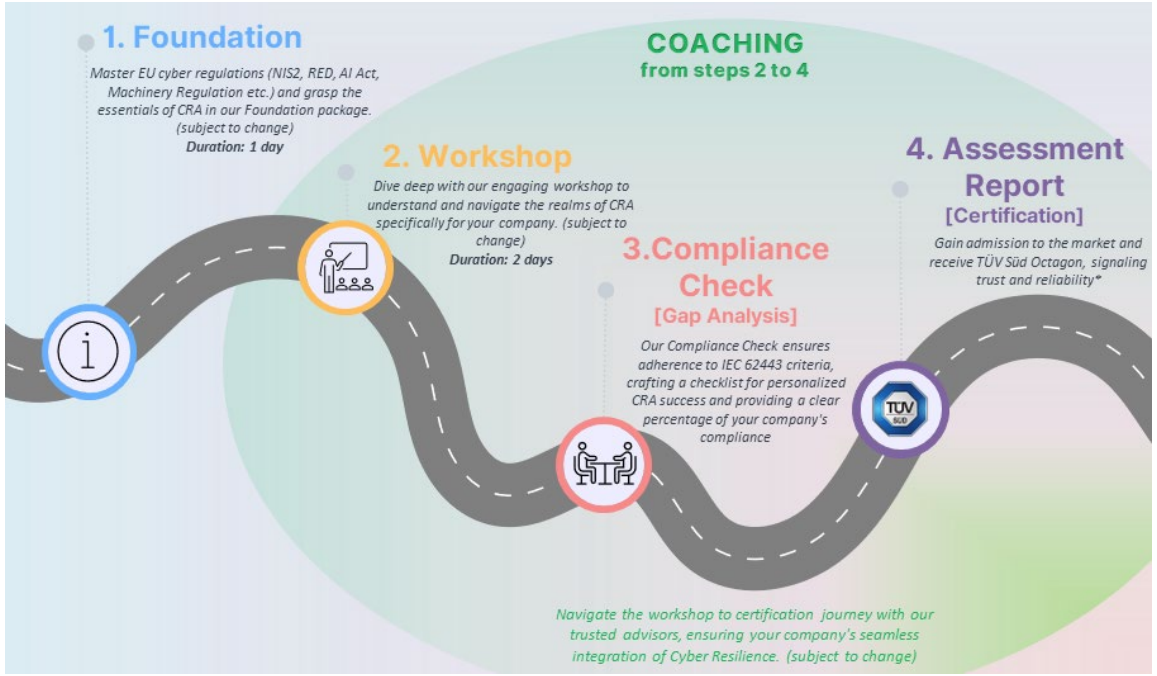


This test-scheme is continuously updated with latest information from

The European Commission and development of harmonized standards.

Road to CRA compliance - preparation

To keep market access for your products it is important to prepare early so that your products can achieve a positive assessment by the notified body.



Knowledge & Strategy

To help you build the strategy TÜV SÜD offers Training, Workshops and Webinars. For details on this visit https://www.tuvsud.com/en/resource-centre/stories/cyber-resilience-act-a-new-era-in-product-cybersecurity

TÜV SÜD can also assist you in the development process with early feedback e.g. to your cybersecurity risk assessment.

Preliminary Testing

Before being appointed as notified body, TÜV SÜD can already carry out conformity assessments, tests and audits according to the latest state of our test-scheme.

By this you can discover gaps and improvement opportunities early in the process. This testing can cover any or all of the areas described here.

Erforderliche Dokumente zur CRA-Konformität

Aktueller vorläufiger Stand der Dokumentation, die TÜV SÜD für die beschriebenen Testbereiche bewertet

- **Geltungsbereich** (Gerätebeschreibung, Klassifizierung nach CRA)
- **Methodik zur Risikobewertung**
  - Identifikation von Risiken
  - Bedrohungsvektoren
  - Tolerierbares Risikoniveau
  - Minderungsstrategie
  - Dokumentenprüfung und -aktualisierung
- **Produktlebenszyklus-Strategie**
- **SBOM** (Software Bill of Materials)
  - Prozess zur Erstellung eines SBOM für jede Version
  - SBOM in maschinenlesbarem Format
- **Schwachstellenmanagement**
  - Koordinierte Offenlegungspolitik
  - Update-Mechanismen
  - Aktualisierungszeitpunkte
- **Tests**
  - Sicherheitstests
  - Prüfung der Sicherheitsimplementierung
- Nutzerinformationen
  - Benutzerhandbuch
  - Etikett, Produktbild, Produktidentifikation, Modell, Seriennummer
  - Bewertung des Cybersicherheitsrisikos (vollständig oder zusammengefasst)
- **Sorgfaltspflicht in der Lieferkette**
  - Bewertung der Lieferanten
  - Integration von Komponenten
- **Nachweise zur regulatorischen Konformität**
  - Konformitätserklärung Technische Dokumentation
  - Alle für die DoC und technische Dokumentation vorgeschriebenen Unterlagen

CE 0123

Wie Sie sich auf den CRA vorbereiten können

- **Prüfen Sie Anhang III und IV des CRA** um zu bestimmen, unter welche Kategorie Ihre Produkte fallen.

- Wenn Ihre Produkte **bereits nach einem Cybersicherheitsstandard entwickelt** wurden, prüfen Sie z. B. **„ENISA – Cyber Resilience Act Requirements Standards Mapping“**, um festzustellen, welche CRA-Anforderungen bereits erfüllt sind.

- **Aktuelle Veröffentlichungen prüfen**, insbesondere von benannten Stellen oder Fachverbänden (z. B. VDMA, VDE).

- Analysieren Sie **Lücken zwischen aktuellen Prozessen/Produkten** und:
  - Den Anforderungen aus dem Gesetzestext
  - Ggf. bestehenden Zertifizierungen wie **EN 303 645** und **IEC 62443**
  - **EN 18031-1, -2 und -3**, da diese als Grundlage für neue Standards dienen sollen

- **Alle erforderlichen Dokumente vorbereiten:**
  - **Konformitätserklärung** (siehe Anhang V und dieses Folienset)
  - **Technische Dokumentation** (Anhang VIII und dieses Folienset)
  - **Benutzerhandbuch** (Anhang II und dieses Folienset)
  - Nachweise zur **Konformität mit allen weiteren CRA-Anforderungen**

- Wenn Ihr Produkt zur **wichtigen oder kritischen Kategorie** gehört, kontaktieren Sie eine **benannte Stelle**, die Sie bei der Vorbereitung unterstützen kann.

In Kurz - Wichtigste Pflichten für Hersteller

- Cybersicherheit über gesamten Produktlebenszyklus
- Sicherheitsbewertung und technische Dokumentation
- CE-Kennzeichnung und Konformitätserklärung
- Meldung von Schwachstellen (innerhalb 24h)

Sämtliche Produkte haben bestimmte grundlegende Sicherheitsanforderungen zu erfüllen

- unter anderem Freiheit von bekannten Schwachstellen, grundsätzliche Updatefähigkeit und Möglichkeit, Updates zu verschieben, Schutz vor unbefugtem Zugriff, Schutzpflichten im Hinblick auf Datenminimierung, Datenprotokollierung, sichere Standardkonfiguration, Erstellen einer Software-Stückliste
- Bekannte Schwachstelle müssen auch dem Hersteller bekannt sein. Aber Achtung: Grob Fahrlässige Nichtkenntnis stellt evtl. auch einen Verstoß gegen den CRA dar
- „Verschiebbarkeit“ des Updates nicht immer sinnvoll
  - Eher ja bei einem selbst gewarteten Server, bei dem ich Updates in einer Sandbox testen kann
  - Eher nein bei technisch nicht versierten Verbrauchern die Updates weder testen noch zurückrollen können

Länge des Unterstützungszeitraums

- Mindestens fünf Jahre (Art. 13 Abs. 8 CRA), es sei denn, das Produkt ist weniger als fünf Jahre in Betrieb, dann voraussichtliche Nutzungsdauer
- Ggf. sinnvolle Anknüpfung an Zeitraum, in dem etwaige Gewährleistungsansprüche geltend gemacht werden können

Sicherheits-Risikobewertung

- Bewertung muss sich auf die gesamte Produktlebensdauer erstrecken (Art. 13 Abs. 2 bis 4 CRA), also alles von der Planungs- bis zur Wartungsphase
- Sicherheitsbewertung geknüpft an den Unterstützungszeitraum

Vielen Dank für Ihr Interesse!

Melden Sie sich gerne mit Ihren Fragen bei uns: sns@tuvsud.com

Kontaktanfragen gerne an:

sns@tuvsud.com

TÜV SÜD

Folgen Sie uns auf:

tuvsud.com
info@tuvsud.com

Anhang III, IV & V

Annex III: Important Products with Digital Elements Class I

1. Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers
2. Standalone and embedded browsers
3. Password managers
4. Software that searches for, removes, or quarantines malicious software
5. Products with digital elements with the function of virtual private network (VPN)
6. Network management systems
7. Security information and event management (SIEM) systems
8. Boot managers
9. Public key infrastructure and digital certificate issuance software
10. Physical and virtual network interfaces
11. Operating systems
12. Routers, modems intended for the connection to the internet, and switches
13. Microprocessors with security-related functionalities
14. Microcontrollers with security-related functionalities
15. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities
16. Smart home general purpose virtual assistants
17. Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems
18. Internet connected toys covered by Directive 2009/48/EC of the European Parliament and of the Council (1) that have social interactive features (e.g. speaking or filming) or that have location tracking features
19. Personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 or (EU) No 2017/746 do not apply, or personal wearable products that are intended for the use by and for children

Annex III: Important Products with Digital Elements Class II

1. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments
2. Firewalls, intrusion detection and prevention systems
3. Tamper-resistant microprocessors
4. Tamper-resistant microcontrollers

Annex IV: Critical Products with Digital Elements

1. Hardware Devices with Security Boxes
2. Smart meter gateways within smart metering systems as defined in Article 2, point (23) of Directive (EU) 2019/944 of the European Parliament and of the Council (1) and other devices for advanced security purposes, including for secure cryptoprocessing
3. Smartcards or similar devices, including secure elements

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 authorized 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

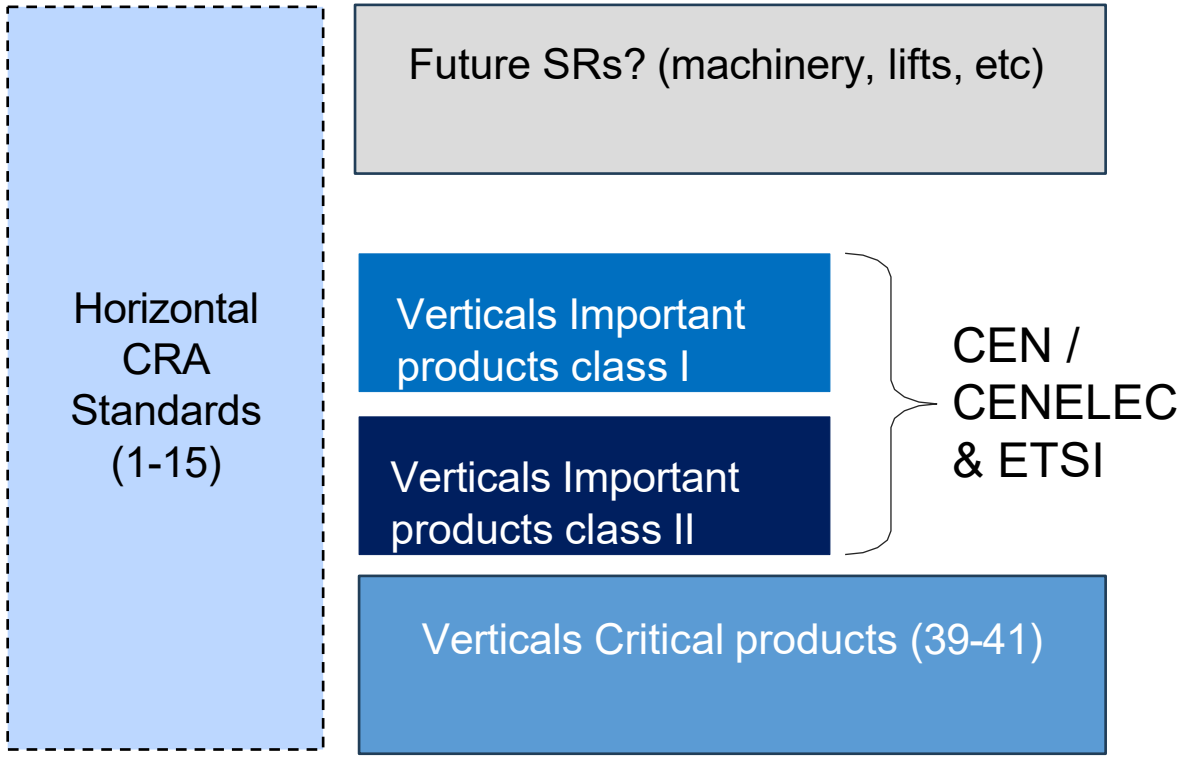
7. Where applicable, the name and number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued

8. Additional information: Signature, name, function, place, date

CRA Standardization Requests

- **Horizontal Framework:** guidance for common security by design consideration, threat modeling, risk assessment
- **Product-agnostic (horizontal) cybersecurity requirements (1-15),** addressing different aspects and mechanisms of product cybersecurity for products with digital elements.
  - ❖ Risk-based approach (CRA Annex I)
  - ❖ Essential Requirements (CRA Annex I part 1)
  - ❖ Vulnerability Handling (CRA Annex I part 2) Splitting the requirements of Annex I-I into 13 standards.
- **Specifications for vulnerability handling processes**, covering all relevant product categories, to be put in place by manufacturers of products with digital elements.
- **Product-specific (vertical) cybersecurity requirements (16-41),** relating to the properties of products with digital elements:
  - ❖ Important products class 1 (CRA Annex III)
  - ❖ Important products class 2 (CRA Annex III)
  - ❖ Critical products (CRA Annex IV)

Requested standards



Standards to be developed

Source: Standardisation Request 2025-02-03

Horizontals

1) Design and development based on risks
2) Make available without exploitable vulnerabilities
3) Secure by default
4) Security updates
5) Access control
6) Data confidentiality
7) Data integrity
8) Data privacy
9) Availability of essential functions
10) Minimize negative impact on other devices
11) Limited attack surface
12) Minimize impact of an incident
13) Monitoring
14) Remove all data
15) Vulnerability handling

Verticals

16) Identity management systems
17) Browsers
18) Password managers
19) Anti-virus
20) VPN
21) Network management
22) SIEM
23) Boot managers
24) Certificate issuance
25) Network interfaces
26) Operating systems
27) Routers & switches
28) Microprocessors
29) Microcontrollers
30) ASIC & FPGA
31) Smart Home assistants
32) Smart home products
33) Internet connected toys
34) Wearable products
35) Hypervisors
36) Firewalls, IDS / IPS
37) Tamper-resistant microprocessors
38) Tamper-resistant microcontrollers
39) Hardware devices with security boxes
40) Smart meter gateways
41) Smartcards & secure elements