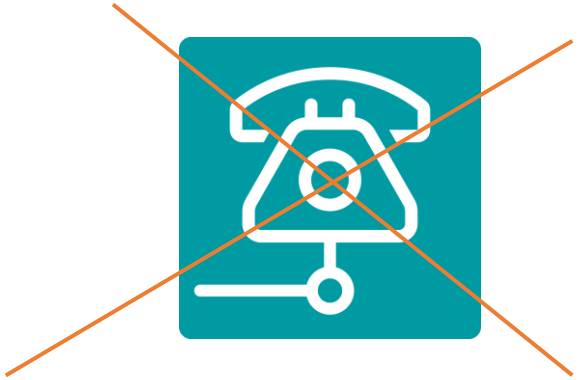
IEC 62443 Cybersecurity Tagung

Cyber Resilience Act – CyberSecurity EU-Richtlinie für Produkte mit digitalen Elementen

Das Committee CEN/CENELEC/JTC 13/WG 9 "Special Working Group on Cyber Resilience Act"

EU Cyber Resilience Act

Hersteller und Importeure sind verpflichtet, für jedes **„Produkt mit digitalen Elementen“** eine EU-Konformitätsbewertung durchzuführen. Ziel dieser Bewertung ist die Sicherstellung der Erfüllung der Cybersicherheitsanforderungen gemäß des Cyber Resilience Acts.



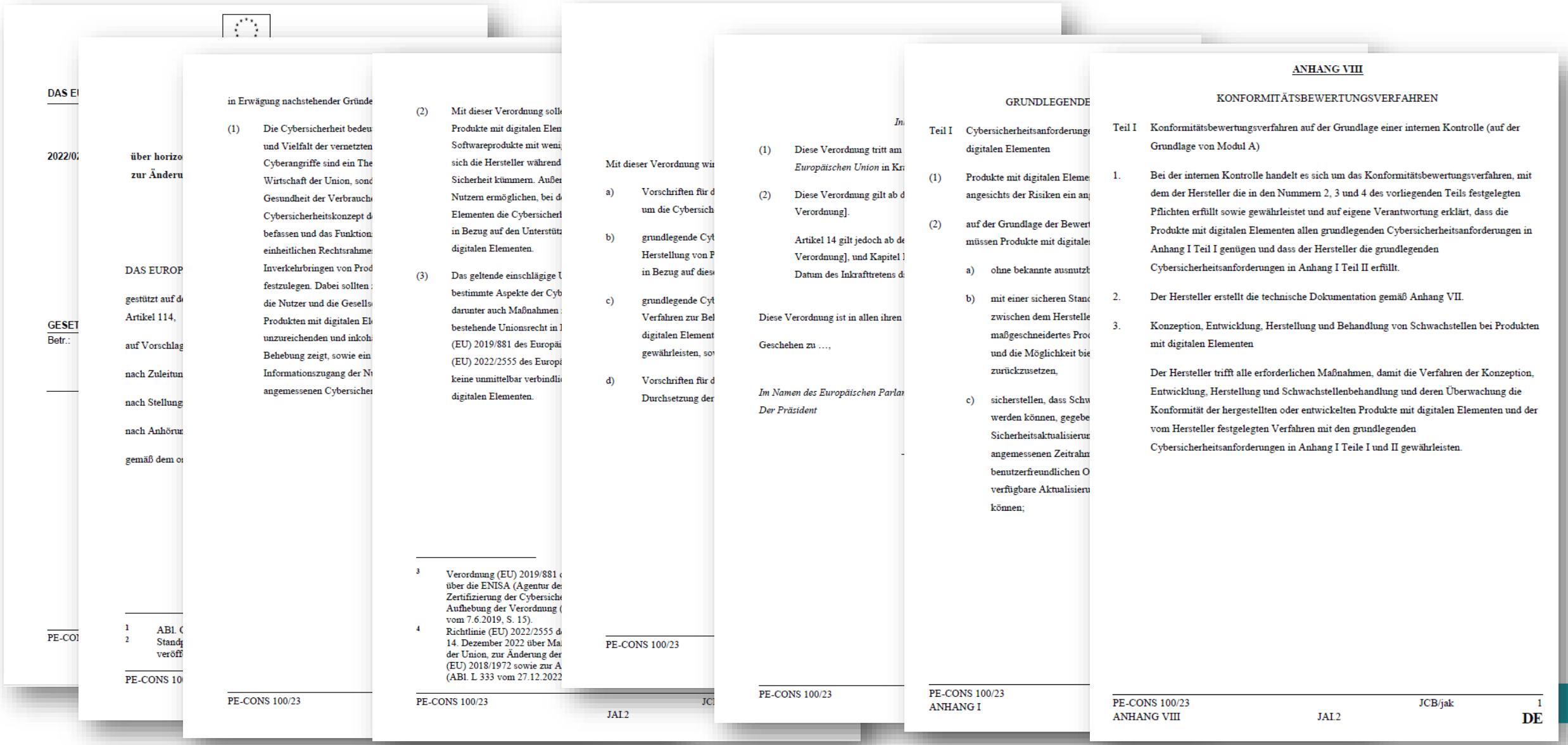
CRA-Richtlinie
(2024/xxx/EU)

„**Produkte mit digitalen Elementen**“ sind alle Produkte, die **digitale Daten verarbeiten, speichern oder übertragen könnten**.

Betroffen sind also alle Produkte, die in der Lage sind, **mit anderen Netzwerken und Geräten, drahtlos, drahtgebunden oder optisch zu kommunizieren**.

Laut Art. 03 (1) des CRA ist dies jedes Software- oder Hardware-Produkt und seine Lösungen zur Datenverarbeitung.

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über
horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen



DAS E

2022/0

über horizo
zur Änderu

DAS EUROP

gestützt auf d
Artikel 114,

GESET
Betr.:

auf Vorschlag

nach Zuleitun

nach Stellung

nach Anhörun

gemäß dem o

PE-CO

1 ABl. C
2 Stand
veröff

PE-CONS 10

in Erwägung nachstehender Gründe

(1) Die Cybersicherheit bedeu
und Vielfalt der vernetzten
Cyberangriffe sind ein The
Wirtschaft der Union, sond
Gesundheit der Verbrauch
Cybersicherheitskonzept d
befassen und das Funktion
einheitlichen Rechtsrahme
Inverkehrbringen von Prod
festzulegen. Dabei sollten
die Nutzer und die Gesells
Produkten mit digitalen El
unzureichenden und inkoh
Behebung zeigt, sowie ein
Informationszugang der N
angemessenen Cybersiche

PE-CONS 100/23

(2) Mit dieser Verordnung soll
Produkte mit digitalen Elem
Softwareprodukte mit weni
sich die Hersteller während
Sicherheit kümmern. Auße
Nutzern ermöglichen, bei d
Elementen die Cybersicherh
in Bezug auf den Unterstütz
digitalen Elementen.

(3) Das geltende einschlägige U
bestimmte Aspekte der Cyb
darunter auch Maßnahmen
bestehende Unionsrecht in
(EU) 2019/881 des Europäi
(EU) 2022/2555 des Europä
keine unmittelbar verbindli
digitalen Elementen.

3 Verordnung (EU) 2019/881
über die ENISA (Agentur de
Zertifizierung der Cybersiche
Aufhebung der Verordnung
vom 7.6.2019, S. 15).
4 Richtlinie (EU) 2022/2555 d
14. Dezember 2022 über Ma
der Union, zur Änderung der
(EU) 2018/1972 sowie zur A
(ABl. L 333 vom 27.12.2022

PE-CONS 100/23

Mit dieser Verordnung wi

a) Vorschriften für d
um die Cybersich

b) grundlegende Cyt
Herstellung von P
in Bezug auf dies

c) grundlegende Cyt
Verfahren zur Bel
digitalen Element
gewährleisten, so

d) Vorschriften für d
Durchsetzung der

PE-CONS 100/23

JAI.2

In

(1) Diese Verordnung tritt am
Europäischen Union in Kr

(2) Diese Verordnung gilt ab d
Verordnung].

Artikel 14 gilt jedoch ab de
Verordnung], und Kapitel I
Datum des Inkrafttretens d

Diese Verordnung ist in allen ihren

Geschehen zu …,

Im Namen des Europäischen Parlam
Der Präsident

PE-CONS 100/23

GRUNDLEGENDE

Teil I Cybersicherheitsanforderunge
digitalen Elementen

(1) Produkte mit digitalen Eleme
angesichts der Risiken ein an

(2) auf der Grundlage der Bewert
müssen Produkte mit digitale

a) ohne bekannte ausnutzt

b) mit einer sicheren Stand
zwischen dem Herstelle
maßgeschneidertes Proc
und die Möglichkeit bie
zurückzusetzen,

c) sicherstellen, dass Schw
werden können, gegebe
Sicherheitsaktualisierun
angemessenen Zeitrahm
benutzerfreundlichen O
verfügbare Aktualisieru
können;

PE-CONS 100/23
ANHANG I

ANHANG VIII

KONFORMITÄTSBEWERTUNGSVERFAHREN

Teil I Konformitätsbewertungsverfahren auf der Grundlage einer internen Kontrolle (auf der Grundlage von Modul A)

1. Bei der internen Kontrolle handelt es sich um das Konformitätsbewertungsverfahren, mit dem der Hersteller die in den Nummern 2, 3 und 4 des vorliegenden Teils festgelegten Pflichten erfüllt sowie gewährleistet und auf eigene Verantwortung erklärt, dass die Produkte mit digitalen Elementen allen grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I genügen und dass der Hersteller die grundlegenden Cybersicherheitsanforderungen in Anhang I Teil II erfüllt.

2. Der Hersteller erstellt die technische Dokumentation gemäß Anhang VII.

3. Konzeption, Entwicklung, Herstellung und Behandlung von Schwachstellen bei Produkten mit digitalen Elementen

Der Hersteller trifft alle erforderlichen Maßnahmen, damit die Verfahren der Konzeption, Entwicklung, Herstellung und Schwachstellenbehandlung und deren Überwachung die Konformität der hergestellten oder entwickelten Produkte mit digitalen Elementen und der vom Hersteller festgelegten Verfahren mit den grundlegenden Cybersicherheitsanforderungen in Anhang I Teile I und II gewährleisten.

PE-CONS 100/23 JCB/jak 1
ANHANG VIII JAI.2 DE

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über
horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen

Design, Entwicklung und Produktion:

- ✓ Design mit limitierter Angriffsfläche (Security by Design)
- ✓ In Verkehr bringen ohne bekannte Schwachstellen
- ✓ Sichere Standardeinstellungen (Auslieferungszustand)

Vulnerability Handling (Umgang mit Sicherheitslücken):

- ✓ Meldung, Behebung und Dokumentation von Schwachstellen
- ✓ Erstellung einer SBOM „Software Bill of Materials“ (Hersteller sind nicht verpflichtet, ihr Software-Stücklisten öffentlich zugänglich zu machen)
- ✓ Es muss eine koordinierte Offenlegungspolitik für Schwachstellen (CSERT, PSERT) geben
- ✓ Kostenlos Bereitstellung von Sicherheitsupdates für bis zu 5 Jahren, insofern die erwartbare Nutzungsdauer nicht kürzer ist

Technische Dokumentation:

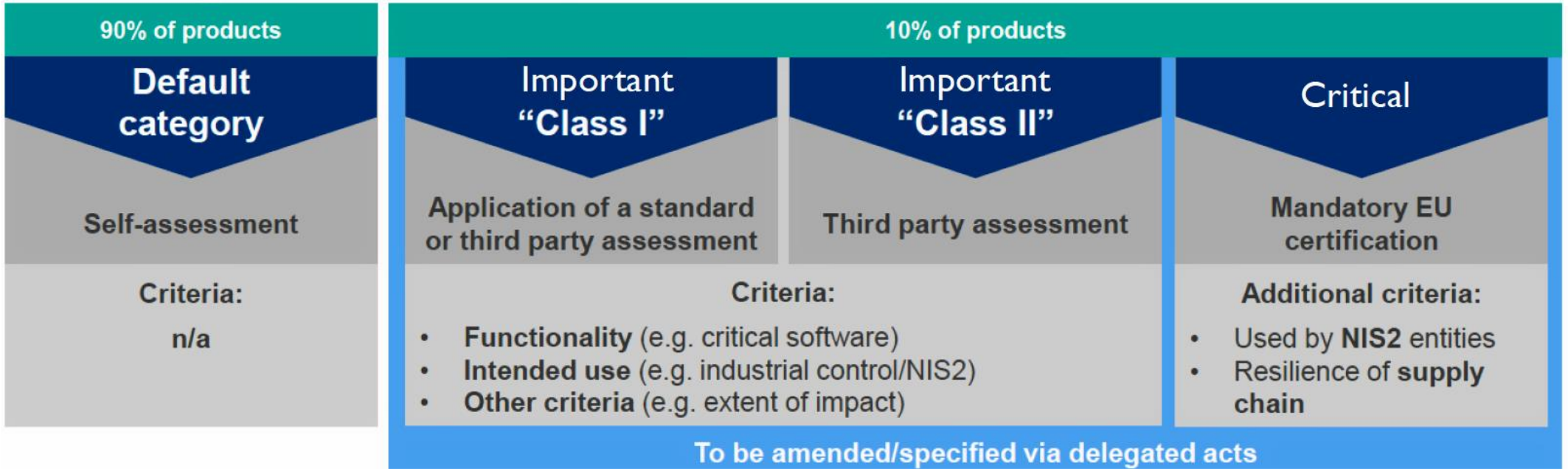
- ✓ Hersteller müssen eine technische Dokumentation erstellen, die Informationen über Design, Entwicklung, Produktion und Schwachstellenmanagement enthält
- ✓ Die Dokumentation muss mindestens 10 Jahre nach dem Inverkehrbringen des Produkts oder für die Dauer des Supportzeitraums aufbewahrt werden

Benachrichtigungspflichten:

- ✓ Aktiv ausgenutzte Schwachstellen und schwerwiegende Vorfälle müssen innerhalb von 24 Stunden an ENIAS und CSERT gemeldet werden
- ✓ Eine detaillierte Berichterstattung über die Schwachstellen und Vorfälle muss innerhalb von 72 Stunden erfolgen

PHOENIX CONTACT

CONFORMITY ASSESSMENT – RISK CATEGORIZATION



Produkte mit digitalen Elementen (Selbsterklärung)	**Wichtige Produkte Anhang III / Klasse I** (Selbsterklärung mit vollständig angewandter hEN)	**Wichtige Produkte Anhang III / Klasse II** (Konformitätsbewertung durch Dritte)	**Kritische Produkte Anhang IV** (EU-Zertifizierungssystem)
Textverarbeitung, Spiele, Smart Speaker, Computer Maus, ...	I.1 Identitätsmanagementsysteme und Software und Hardware für die Verwaltung privilegierter Zugriffe, einschließlich Lesegeräte für die Authentifizierung und Zugangskontrolle, einschließlich biometrischer Lesegeräte …… I.17 Smart-Home-Produkte mit Sicherheitsfunktionen, darunter intelligente Türschlösser, Sicherheitskameras, Babyüberwachungssysteme und Alarmsysteme	II.1 Hypervisoren und Container-Laufzeitsysteme, die die virtualisierte Ausführung von Betriebssystemen und ähnlichen Umgebungen unterstützen II.2 Firewalls, Angriffserkennungs- und/oder -präventionssysteme II.3 Manipulationssichere Mikroprozessoren II.4 Manipulationssichere Mikrocontroller	C.1 Hardwaregeräte mit Sicherheitsboxen C.2 Smart Meter Gateways innerhalb intelligenter Messsysteme im Sinne von Artikel 2 (23) der Richtlinie (EU) 2019/944 und andere Geräte für erweiterte Sicherheitszwecke, einschließlich für sichere Kryptoverarbeitung C.3 Smartcards oder ähnliche Geräte, einschließlich sicherer Elemente

CONFORMITY ASSESSMENT – RISK CATEGORIZATION

Products with digital elements Art. 3 (1)	**Important products with digital elements** Annex III Class 1	**Important products with digital elements** Annex III Class 2	**Critical products with digital elements** Annex IV
Modul A (Interne Fertigungskontrolle) umfasst die Selbstbewertung, d.h. der Hersteller bewertet ohne Beteiligung einer notifizierten Stelle die Konformität seines Produktes.	Anwendung von harmonisierten Normen: **Modul A** (Interne Fertigungskontrolle) umfasst die Selbstbewertung, d.h. der Hersteller bewertet ohne Beteiligung einer notifizierten Stelle die Konformität seines Produktes. oder EU-Cybersicherheitszertifikat nach VO (EU) 2019/881 – VW-Stufe „niedrig“	Anwendung von harmonisierten Normen: **Modul B** (Baumusterprüfung) oder **H** (Umfassende Qualitätssicherung) bewertet die notifizierte Stelle die Qualitätssicherung des Herstellers, d.h. die **notifizierte Stelle überprüft, ob der Qualitätssicherungs-prozess des Herstellers** zu Produkten führt, die mit dem CRA konform sind. oder EU-Cybersicherheitszertifikat nach VO (EU) 2019/881 – VW-Stufe „mittel“	**Zertifizierung nach Verordnung (EU) 2019/881** („Cybersecurity Act“) Vertrauenswürdigkeitsstufen „hoch“ Konformitätsbewertungsstelle „hoch“ Z.z.t. Zertifizierung bei einer nationalen Behörde für die Cybersicherheits-zertifizierungen European Union Common Criteria Scheme (EUCC)
Art. 6 Art. 32 **(1)** Annex VIII Teil 1	Art. 7 Art. 32 **(2)** Annex VIII Teil 2&3	Art. 7 Art. 32 **(3)** Annex VIII Teil 2&3	Art. 8 Art. 32 **(4)** Annex VIII Teil 2&3

Produkte mit digitalen Elementen (Selbsterklärung)	**Wichtige Produkte Anhang III / Klasse I** (Selbsterklärung mit vollständig angewandter hEN)	**Wichtige Produkte Anhang III / Klasse II** (Konformitätsbewertung durch Dritte)	**Kritische Produkte Anhang IV** (EU-Zertifizierungssystem)
Textverarbeitung, Spiele, Smart Speaker, Computer Maus, ...	I.1 Identitätsmanagementsysteme und Software und Hardware für die Verwaltung privilegierter Zugriffe, einschließlich Lesegeräte für die Authentifizierung und Zugangskontrolle, einschließlich biometrischer Lesegeräte …… I.17 Smart-Home-Produkte mit Sicherheitsfunktionen, darunter intelligente Türschlösser, Sicherheitskameras, Babyüberwachungssysteme und Alarmsysteme	II.1 Hypervisoren und Container-Laufzeitsysteme, die die virtualisierte Ausführung von Betriebssystemen und ähnlichen Umgebungen unterstützen II.2 Firewalls, Angriffserkennungs- und/oder -präventionssysteme II.3 Manipulationssichere Mikroprozessoren II.4 Manipulationssichere Mikrocontroller	C.1 Hardwaregeräte mit Sicherheitsboxen C.2 Smart Meter Gateways innerhalb intelligenter Messsysteme im Sinne von Artikel 2 (23) der Richtlinie (EU) 2019/944 und andere Geräte für erweiterte Sicherheitszwecke, einschließlich für sichere Kryptoverarbeitung C.3 Smartcards oder ähnliche Geräte, einschließlich sicherer Elemente

EU-Konformitätsbewertung

58.03.003.0131 DoC-202009-17

EU-Konformitätserklärung (DE)

Hersteller: REOLINK INNOVATION LIMITED
Adresse: Room B,4th Floor, Kingway Commercial Building, 171-173 Lockhart Road, Wan Chai, Hong Kong

Diese Konformitätserklärung wurde unter der alleinigen Verantwortung des Herstellers ausgestellt und gehört zum folgenden Produkt:
Produkttyp: IP-Kamera
Modell: RLC-810A, RLC-510A

Das oben beschriebene Objekt der Erklärung entspricht den betreffenden Harmonisierungsrechtsvorschriften der Union:
- EMV-Richtlinie: 2014/30/EU
- RoHS-Richtlinie: 2011/65/EU

Die folgenden harmonisierten Normen und technischen Spezifikationen wurden angewendet:

EMV	EN 55032:2015, EN 55035: 2017
RoHS	EN 50581:2012

Unterzeichnet für und im Namen von: REOLINK INNOVATION LIMITED

Ausstellungsort: Hong Kong
Ausstellungsdatum: 25-9-2020
Name: Wang aijun
Funktion: Technischer Direktor
Unterschrift:

Wang aijun

EMV-Richtlinie 2014/30/EU Elektromagnetische Verträglichkeit von Elektro- und Elektronikprodukten

- **IEC/EN 55032** ist eine Emissionsnorm
- **IEC/EN 55035** ist ein Störfestigkeitsstandard

RoHS-Richtlinie 2011/65/EU
zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronik-geräten

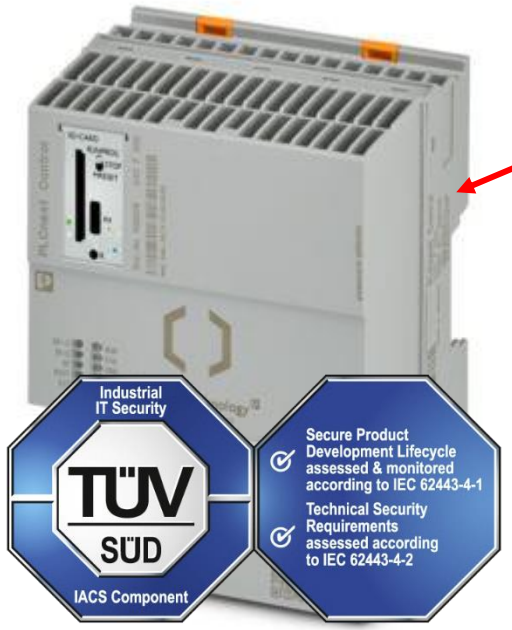
- **IEC/EN 50581** zur Technische Dokumentation und Beurteilung von Elektro- und Elektronikgeräten hinsichtlich der Beschränkung gefährlicher Stoffe

*Seit dem 18.11.2021 ist die Europäische Norm DIN EN **50581:2012** ausgelaufen und durch die harmonisierte Norm **IEC/EN 63000:2018** ersetzt worden.*

***CRA-Richtlinie 2024/xxx/EU** Cyber Resilienz für Produkt mit digitalen Elementen*

- ***IEC/EN 62443-4-1** Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung*
- ***IEC/EN 62443-4-2** Technische Sicherheitsanforderungen an IACS-Komponenten*

EU-Konformitätsbewertung



Tested according to:

IEC 62443-4-1 (Full LM3 Process Profil)

Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung

IEC 62443-4-2 (Scurity Level 2)

Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme

PHOENIX CONTACT

EU-Konformitätserklärung Nr. 2866763.CE.05
EU-Declaration of Conformity No.

Hersteller / *Manufacturer*: PHOENIX CONTACT GMBH & CO. KG
Anschrift / *Address*: Flachsmarktstraße 8, D-32825 Blomberg, Germany

Produktbezeichnung / *Product description*:
(Artikelbezeichnung, / *Article description*, Artikel-Nr. / *Article no.*)

Das vorstehend bezeichnete Produkt stimmt mit den wesentlichen Anforderungen der nachfolgenden Richtlinie(n) und deren Änderungsrichtlinien überein / *The above mentioned product is in line with the essential requirements of the below directive(s) and their modification directive(s):*

2014/30/EU	EMV-Richtlinie (Elektromagnetische Verträglichkeit) Electromagnetic Compatibility Directive (EMC)
2014/35/EU	Niederspannungs-Richtlinie Low Voltage Directive (LVD)

Für die Beurteilung der Übereinstimmung wurden folgende einschlägige Normen herangezogen:
For evaluation of the conformity following relevant standards were consulted:

EN 60950-1:2006+A11:2009+A1:2010+A12:2011 | EN 61000-3-2:2006+A1:2009+A2:2009 | EN 61000-6-2:2005
EN 61000-6-3:2007+A1:2011

Weitere Informationen (z. B. Dokumente, Prüfberichte, Einschränkungen, etc.) zur Konformitätsbewertung:
Additional information (for example documents, test reports, restrictions etc.,) of the conformity assessment:

Zertifikate einer benannten Stelle / *Certificates by a notified body*:
Anschrift / *Address*:
Referenz / *Reference*:
Anschrift / *Address*:
Referenz / *Reference*:

Die letzten beiden Ziffern des Jahres in dem die CE-Kennzeichnung angebracht wurde: 07
The last two figures of the year in which the CE marking was applied:
(nur einzutragen, bei der Niederspannungsrichtlinie / *only to be entered on the low voltage directive*)

☒ Diese Erklärung gilt auch für die im Anhang aufgelisteten Produkte. (wenn angekreuzt)
This declaration also applies for the products listed in the annex. (If marked with a cross)

Diese Erklärung bescheinigt die Übereinstimmung mit den wesentlichen Anforderungen der genannten Richtlinie(n), enthält jedoch keine Zusicherung von Eigenschaften. Die Sicherheits- und Einbauhinweise der mitgelieferten Produktdokumentation sind zu beachten.
This declaration certifies the conformity with the essential requirements of the indicated directive(s), it does not, however, covenant any characteristics. The instructions for safety and installation of the enclosed product documentation have to be observed.

Blomberg, 2016-04-20

i. A. Werner Meyer
PHOENIX CONTACT Power Supplies GmbH
Development Power Supplies
Ansprechpartner / contact person

i. A. Dr.-Ing. Mathias Emsermann
PHOENIX CONTACT Power Supplies GmbH
Vice President
Zeichnungsberechtigter / authorized signatory

FS A-07-0037 / -13-, FS K-7-0013 / -13- 2866763.CE.05 | Formblatterstelldatum / *Date of form establishment*: 2016-04-19 | Formblattersteller / *Form establisher*: Corporate Quality Management | Blatt / *Page* 1 von / *of* 2

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Product Service

CERTIFICATE
No. IITS2 029429 0027 Rev. 02

Holder of Certificate: PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstr. 8
32825 Blomberg
GERMANY

Certification Mark:

Product Type: IACS components

Model(s): PLCnext Control (Configuration: Security Profile active)
AXC F 1152, AXC F 2152, AXC F 3152, AXC F XT SPLC 1000, RFC 4072S, NFC 482S, BPC 9102S

Tested according to: IEC 62443-4-1:2018
IEC 62443-4-2:2019
PPP 15003B:2021 (IEC 62443-4-1: Full ML3 Process Profile)

The secure development lifecycle and the resulting product(s) were assessed on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition, the certification holder must not transfer the certificate to third parties. See http://www.tuvsud.com/ps-cert for details.

Test report no.: 713296124-04
Valid until: 2026-07-25

Date, 2023-08-04 (Michael Hermes)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany
TÜV®

TÜV DEKRA GTÜ CERTIFICATION

PHOENIX CONTACT

Über **100.000** innovative Produkte

11 Produktionsstandorte

Deutschland | China | Taiwan | Indien | Polen | Schweden | Schweiz | Türkei | Argentinien Griechenland | USA

Hauptsitz des Unternehmens: Blomberg, Nordrhein-Westfalen, Deutschland | Umsatz weltweit: 3,4 Milliarden Euro (Stand 2023) | Mitarbeitende weltweit: 21.000

EU Cyber Resilience Act

Industrial IoT-Security Specialist

Normungsgremien:

ASI - Austrian Standards International

ISO-Expert der AG 001.27 Information Security, Cybersecurity and Privacy Protection
CEN/CLC/JTC 13 - Cybersecurity and Data Protection
Delegiert - JTC 13/WG 9 "Special Working Group on Cyber Resilience Act"

OVE - Österreichischer Verband für Elektrotechnik

IEC-Expert TSK MR65 Industrielle Prozess-, Mess-, Regelungs- u. Steuerungstechnik
Stellv. Vorsitzender OVE AG MR65 Industrial Automation & Control Systems Security (z.B. **IEC 62443**)
TSK MR57 Netzleittechnik und zugehörige Übertragungstechnik (Energiewirtschaft)

Über **100.000** innovative Produkte

Unternehmens Zertifizierung in Österreich:

IEC 62443-2-4

Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme

CERTIFICATE

No. IITS1 029429 0015 Rev. 03

Holder of Certificate: PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstr. 8
32825 Blomberg
GERMANY

Certification Mark:

Type: Industrial IT Security

Scope of Certificate: ICS Security Service Provider

Applied Standard(s): IEC 62443-2-4:2015/AMD1:2017
PPP 15010B:2021 (IEC 62443-2-4 ML2 Process Profile for a Generic Service Provider)

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report.
See http://www.tuvsud.com/ps-cert for details.

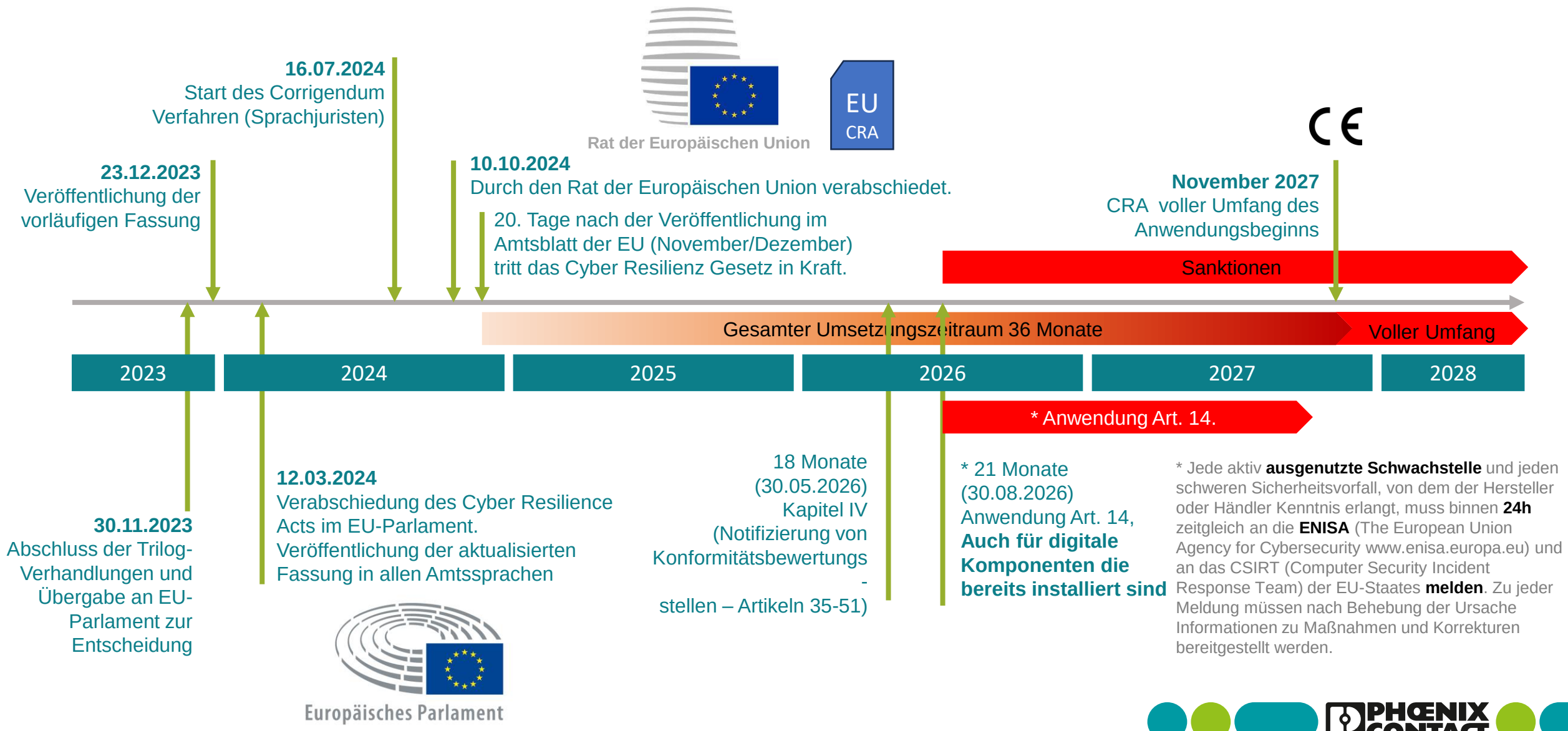
Report No.: 713300933-03

Valid until: 2026-07-25

Date, 2023-10-31 (Michael Hermes)

Page 1 of 2
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

EU Cyber Resilience Act – Zeitplan



* Jede aktiv **ausgenutzte Schwachstelle** und jeden schweren Sicherheitsvorfall, von dem der Hersteller oder Händler Kenntnis erlangt, muss binnen **24h** zeitgleich an die **ENISA** (The European Union Agency for Cybersecurity www.enisa.europa.eu) und an das CSIRT (Computer Security Incident Response Team) der EU-Staates **melden**. Zu jeder Meldung müssen nach Behebung der Ursache Informationen zu Maßnahmen und Korrekturen bereitgestellt werden.

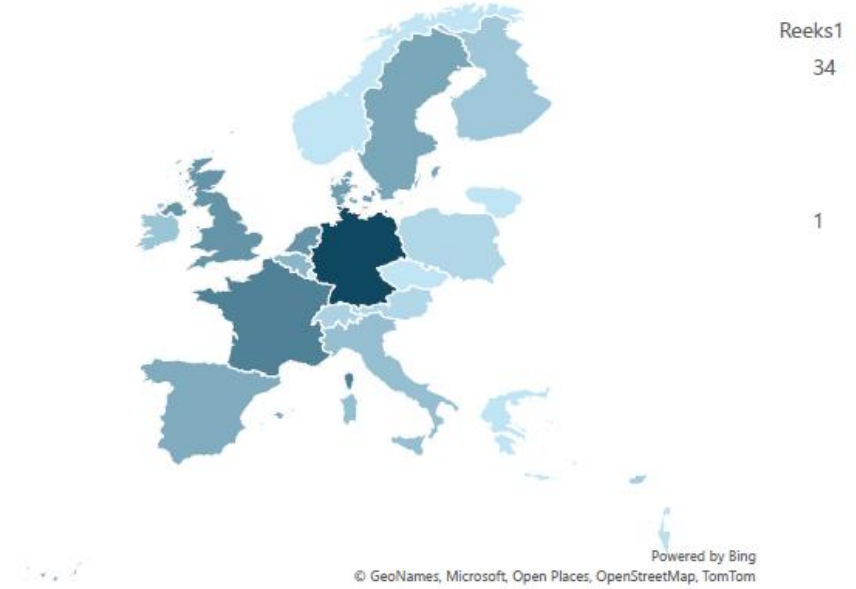
PHOENIX CONTACT

CEN-CENELEC JTC 13/WG 9 Special Working Group on Cyber Resilience Act

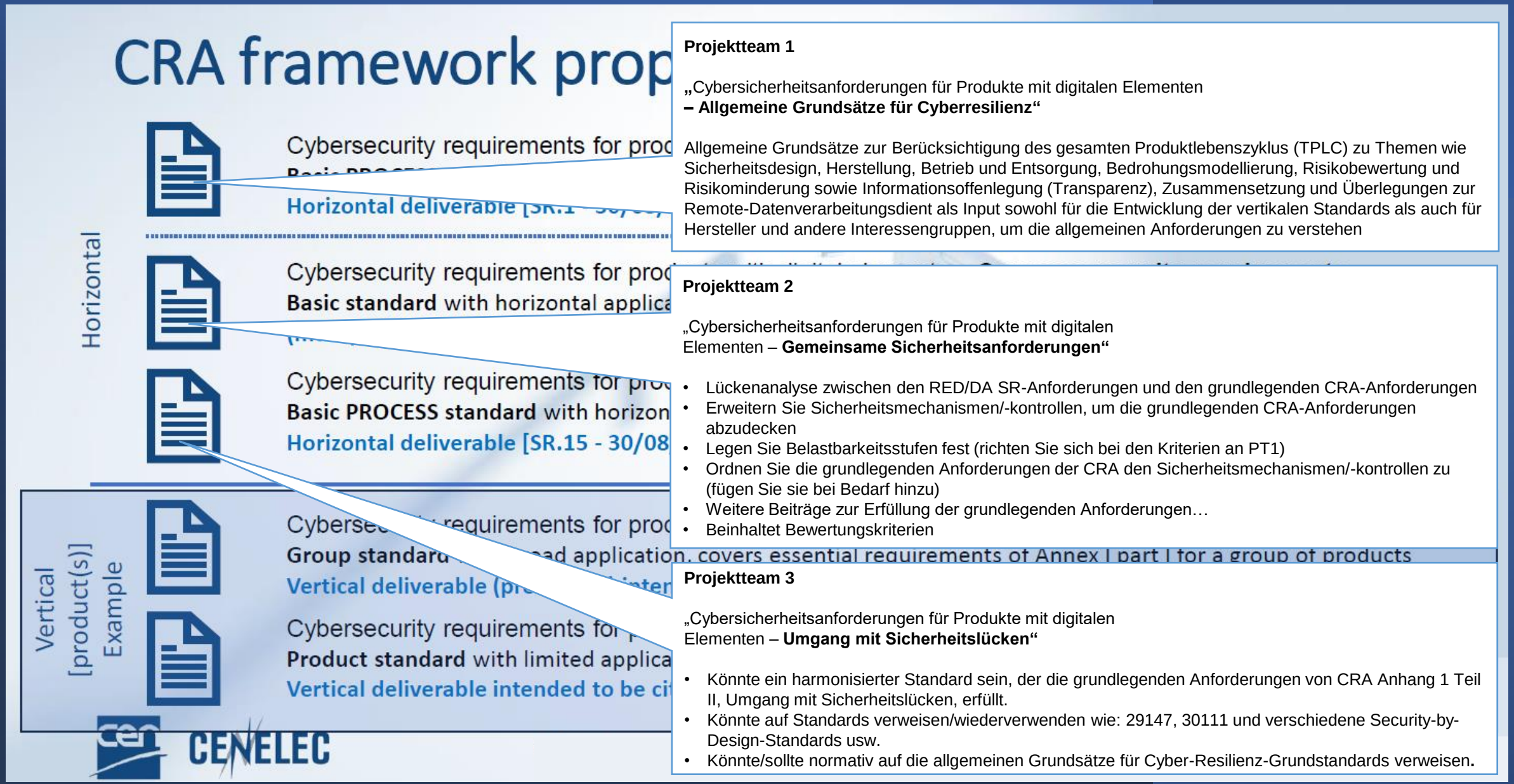
Europäisches Komitee für Normung /

Europäisches Komitee für elektrotechnische Normung

- Established on June 7, 2023.
- Secretariat: NEN, Convenor: Ben Kokx
- Currently 213 committee members representing 20 National Bodies and 12 liaisons/partners



- On a bi-weekly 2.5 hours meeting schedule with 3 day face-to-face / hybrid meetings planned every 2 months
- **JTC 13/WG 9 is focusing on the horizontal standards to address the essential requirements of Annex I *!***



Projektteam 1

„Cybersicherheitsanforderungen für Produkte mit digitalen Elementen
– Allgemeine Grundsätze für Cyberresilienz“

Allgemeine Grundsätze zur Berücksichtigung des gesamten Produktlebenszyklus (TPLC) zu Themen wie Sicherheitsdesign, Herstellung, Betrieb und Entsorgung, Bedrohungsmodellierung, Risikobewertung und Risikominderung sowie Informationsoffenlegung (Transparenz), Zusammensetzung und Überlegungen zur Remote-Datenverarbeitungsdient als Input sowohl für die Entwicklung der vertikalen Standards als auch für Hersteller und andere Interessengruppen, um die allgemeinen Anforderungen zu verstehen

Projektteam 2

„Cybersicherheitsanforderungen für Produkte mit digitalen Elementen – **Gemeinsame Sicherheitsanforderungen“**

- Lückenanalyse zwischen den RED/DA SR-Anforderungen und den grundlegenden CRA-Anforderungen
- Erweitern Sie Sicherheitsmechanismen/-kontrollen, um die grundlegenden CRA-Anforderungen abzudecken
- Legen Sie Belastbarkeitsstufen fest (richten Sie sich bei den Kriterien an PT1)
- Ordnen Sie die grundlegenden Anforderungen der CRA den Sicherheitsmechanismen/-kontrollen zu (fügen Sie sie bei Bedarf hinzu)
- Weitere Beiträge zur Erfüllung der grundlegenden Anforderungen…
- Beinhaltet Bewertungskriterien

Projektteam 3

„Cybersicherheitsanforderungen für Produkte mit digitalen Elementen – **Umgang mit Sicherheitslücken“**

- Könnte ein harmonisierter Standard sein, der die grundlegenden Anforderungen von CRA Anhang 1 Teil II, Umgang mit Sicherheitslücken, erfüllt.
- Könnte auf Standards verweisen/wiederverwenden wie: 29147, 30111 und verschiedene Security-by-Design-Standards usw.
- Könnte/sollte normativ auf die allgemeinen Grundsätze für Cyber-Resilienz-Grundstandards verweisen**.**

2 horizontale Prozessstandards (Anhang I, Teil I) bis 30.08.2026

13 horizontale wesentliche Anforderungen (Anhang I, Teil I) bis 30.10.2027

EUROPEAN COMMISSION
Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Ecosystems III: Construction, Machinery and Standardisation
Standards Policy

Brussels, 16.4.2024

A Notification under Article 12 of Regulation (EU) No 1025/2012[1]

Themen	Beschreibung Horizontal Normen für Sicherheit Anforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen	Fristen	Zuteilung
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	JTC 13 WG9 PT1
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	JTC 13 WG9 PT2
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	JT JTC 13 WG9 PT2
4.	European standard(s) and/or European standardisation deliverable(s) on ensuring that vulnerabilities in products with digital elements can be addressed through security updates	30.10.2027	JTC 13 WG9 PT2
5.	European standard(s) and/or European standardisation deliverable(s) on ensuring protection of products with digital elements from unauthorised access and reporting on possible unauthorised access	30.10.2027	JTC 13 WG9 PT2
6.	European standard(s) and/or European standardisation deliverable(s) on protecting the confidentiality of data stored, transmitted or otherwise processed by a product with digital elements	30.10.2027	JTC 13 WG9 PT2
7.	European standard(s) and/or European standardisation deliverable(s) on protecting the integrity of data, commands, programs by a product with digital elements, and its configuration against any manipulation or modification not authorised by the user, as well as reporting on corruptions	30.10.2027	JTC 13 WG9 PT2
8.	European standard(s) and/or European standardisation deliverable(s) on processing only personal or other data that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements ('minimisation of data')	30.10.2027	JTC 13 WG9 PT2
9.	European standard(s) and/or European standardisation deliverable(s) on protecting the availability of essential and basic functions of the product with digital elements	30.10.2027	JTC 13 WG9 PT2
10.	European standard(s) and/or European standardisation deliverable(s) on minimising the negative impact of a product with digital elements or its connected devices on the availability of services provided by other devices or networks	30.10.2027	JTC 13 WG9 PT2
11.	European standard(s)and/or European standardisation deliverable(s) on designing, developing and producing products with digital elements with limited attack surfaces	30.10.2027	JTC 13 WG9 PT2
12.	European standard(s) and/or European standardisation deliverable(s) on designing, developing and producing products with digital elements that reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques	30.10.2027	JTC 13 WG9 PT2
13.	European standard(s) and/or European standardisation deliverable(s) on providing security related information by recording and/or monitoring relevant internal activity of products with digital elements with an opt-out mechanism for the user	30.10.2027	JTC 13 WG9 PT2
14.	European standard(s) and/or European standardisation deliverable(s) on securely and easily removing or transferring all data and settings of a product with digital elements.	30.10.2027	JTC 13 WG9 PT2
	Horizontale Standards für Anforderungen zum Umgang mit Schwachstellen		
15.	European standard(s) and/or European standardisation deliverable(s) on vulnerability handling for products with digital elements	30.08.2026	JTC 13 WG9 PT3

Draft standardisation request to European Standards Organisations in support of Union policy on cybersecurity requirements for products with digital elements

26 vertikale Standards (Anhang I, Teil I) bis zum 30.10.2026

Thema	Beschreibung
16.	European standa identity manage access control re
17.	European standa standalone and e
18.	European standa password manag
19.	European standa software that se
20.	European standa products with di
21.	European standa network manage
22.	European standa Security informa
23.	European standa managers
24.	European standa key infrastructur

25.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for physical and virtual network interfaces	Last discussion: 2024-06-24 & 2024-07-01 ETSI TC Cyber, Open Source, CLC/TC 65X Layer 1 or 2 Nothing pre-existing; Describe the state of the art Bluetooth, IEEE (Wifi), NFC,...
26.	European stanc operating syste	
27.	European stanc routers, moden	
28.	European stanc microprocessor	
29.	European stanc microcontroller	
30.	European stanc application spe functionalities	
31.	European stanc home general p	
32.	European stanc home products alarm systems	
33.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for Internet connected toys covered by Directive 2009/48/EC that have social interactive features (e.g. speaking or filming) or that have location tracking features	Last discussion: 2024-07-08 3 CEN/TC 52 (?),JTC 13 WG 8, + ETSI TC Cyber **To be discussed with ETSI**
34.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for 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 Regulation (EU) 2017/746 do not apply or personal wearable products that are intended for the use by and for children	Last discussion: 2024-07-08 3 CLC/TC 62 + IEEE + ETSI TC Cyber (?)TC SET and TC SmartBAN, JTC 13 WG 3, WG 8 ISO/IEC JTC 1 SC 17 **To be discussed with ETSI**
35.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments	Potentially *CEN-CLC/JTC 13 WG 6 (to be discussed with ETSI)* (link to EISMEA funding) Experts are available and work needs to be done to bring the experts together, the EISMEA call brings additional resources to support this development.
36.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for firewalls, intrusion detection and/or prevention systems, including specifically those intended for industrial use	Last discussion: 2024-06-17 *CLC/TC 65X WG3* (link to EISMEA funding)
37.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for tamper- resistant microprocessors	Last discussion: 2024-06-10 **CLC TC/47X** (link to EISMEA funding)
38.	erable(s) on essential cybersecurity requirements for	Last discussion: 2024-06-10 **CLC TC/47X** (link to EISMEA funding)
39.	European standard(s) and/or European standardisation deliverable(s) on essential cybersecurity requirements for Hardware Devices with Security Boxes	Last discussion: 2024-06-10 **CEN/TC 224 WG 17** (liaison with CLC/TC 47X if needed) (link to EISMEA funding)
40.	(s) c e 2 ing	
41.	(s) c	(link to EISMEA funding)

EU Cybersicherheit Zertifikat nach VO (EU) 2019/881 „Cybersecurity Act“

Hardware Devices with Security Boxes

- Smart Terminals
- Smart Meters
- Hardware Security Modules (HSM)

Technical Committees

CEN/TC 224 - Machine-readable cards, related device interfaces and operations

WG 17 - Protection Profiles in the context of secure signature creation devices

Draft standardisation request to European Standards Organisations in support of Union policy on cybersecurity requirements for products with digital elements

EU- Rechtsakt zur Cyber Resilienz

CRA-relevante Teile der (EN) IEC 62443-Reihe

- **EN IEC 62443-4-1 „Anforderungen an den sicheren Produktentwicklungslebenszyklus“**
  - Verbindliche Anwendung für EN IEC 62443-4-2
  - EU CRA Anhang I Teil I (1) und Teil II Grundlegende Cybersicherheitsanforderungen
- **EN IEC 62443-4-2 „Technische Sicherheitsanforderungen an IACS-Komponenten“**
  - Umfang: „Produkt“ = (IACS)-Komponenten
  - Anwendung der EN IEC 62443-4-1 verpflichtend
  - EU CRA Anhang I Teil I (2) Grundlegende Cybersicherheitsanforderungen
- **EN IEC 62443-3-3 „Systemsicherheitsanforderungen und Sicherheitsstufen“**
  - Geltungsbereich: „Produkt“ = (Steuerungs-)System (inkl. Maschinen), bestehend aus (IACS-)Komponenten
  - EU CRA Anhang I Teil I (2) Grundlegende Cybersicherheitsanforderungen ab
- IEC 62443-6-2 „Methodik zur Sicherheitsbewertung für IEC 62443-4-2“ (Entwurf)
  - sicheren Produktentwicklungszyklus gemäß IEC 62443-4-1 umgesetzt wurden
- IEC 62443-1-5 „Schema für IEC 62443-Security Profile“
  - Vorgehensweise zum Festlegen von “Security Profile”

Bundesamt
für Sicherheit in der
Informationstechnik

BSI TR-03183 Cyber-Resilienz-Anforderungen

Die Technische Richtlinie TR-03183: Cyber-Resilienz-Anforderungen an Hersteller und Produkte hat zum Ziel, Herstellern schon vorab die Art der Anforderungen, die mit dem künftigen Cyber Resilience Act (Cyber Resilience Act) auf sie zukommen, zugänglich zu machen. Der Cyber Resilience Act wurde als Entwurf der EU-Kommission im September 2022 veröffentlicht und befindet sich derzeit im Gesetzgebungsverfahren. Im Nachgang möglicher Änderungen am Cyber Resilience Act im Vergleich zum Entwurfstext kann auch die Technische Richtlinie aktualisiert werden.

In Teil 1 "General Requirements" werden Anforderungen an Hersteller und Produkte in Anlehnung an die Anforderungen aus Artikeln und Anhängen des Cyber Resilience Act zusammengestellt.

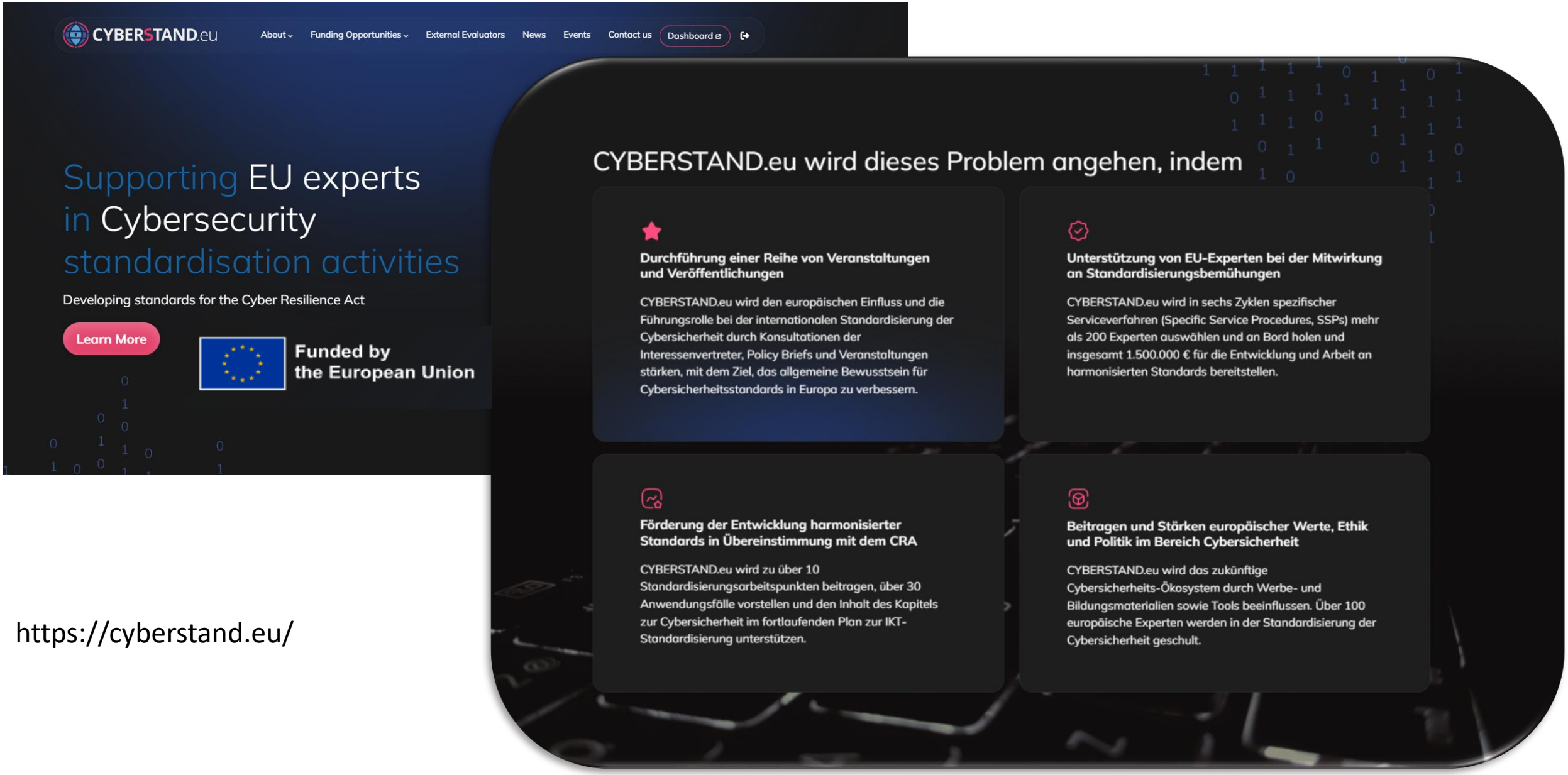
In Teil 2 "Software Bill of Materials (SBOM)" werden formelle und fachliche Vorgaben für Software Bill of Materials beschrieben.

In Teil 3 "Vulnerability Reports and Notifications" wird der Umgang mit eingehenden Schwachstellenmeldungen beschrieben.

Teil 1 und Teil 3 sind als Community Drafts veröffentlicht. Das Fachpublikum ist eingeladen bis zum 30. November 2024 Kommentare und Rückmeldungen an tr03183@bsi.bund.de zu senden.

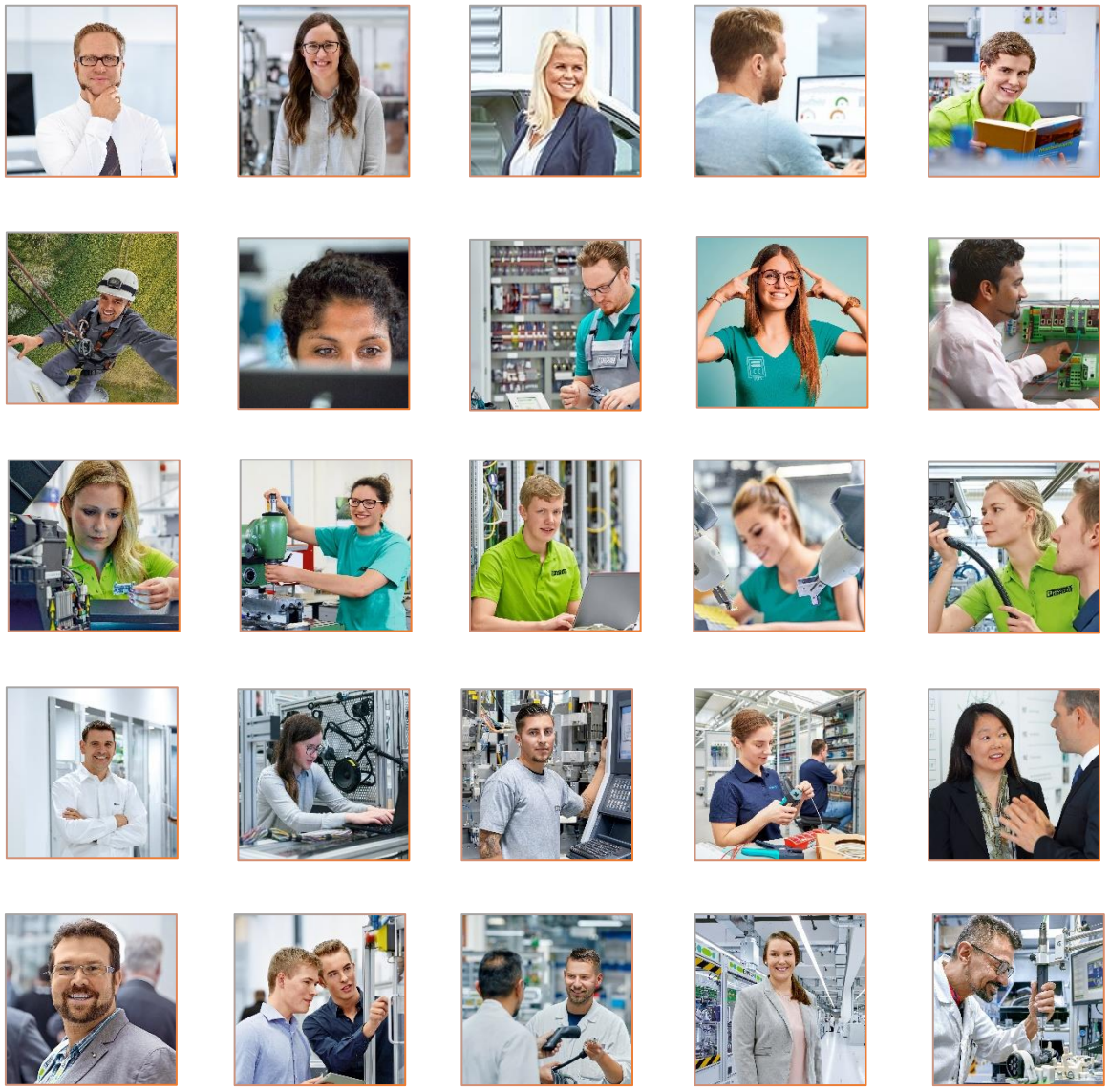
PHOENIX CONTACT

https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03183/TR-03183_node.html



https://cyberstand.eu/

Cyber Resilience Act Working Group (CRAWGs)



…für Ihre Zeit und Ihr Interesse

CRA - Pflichten der Hersteller und Importeure

» Produkte sind in Übereinstimmung mit den grundlegenden Anforderungen von Anhang I zu entwerfen, zu entwickeln und herzustellen

» Erstellung einer technischen Dokumentation

» Beachtung der Sorgfaltspflicht bei der Integration von Komponenten, die von Dritten bezogen werden

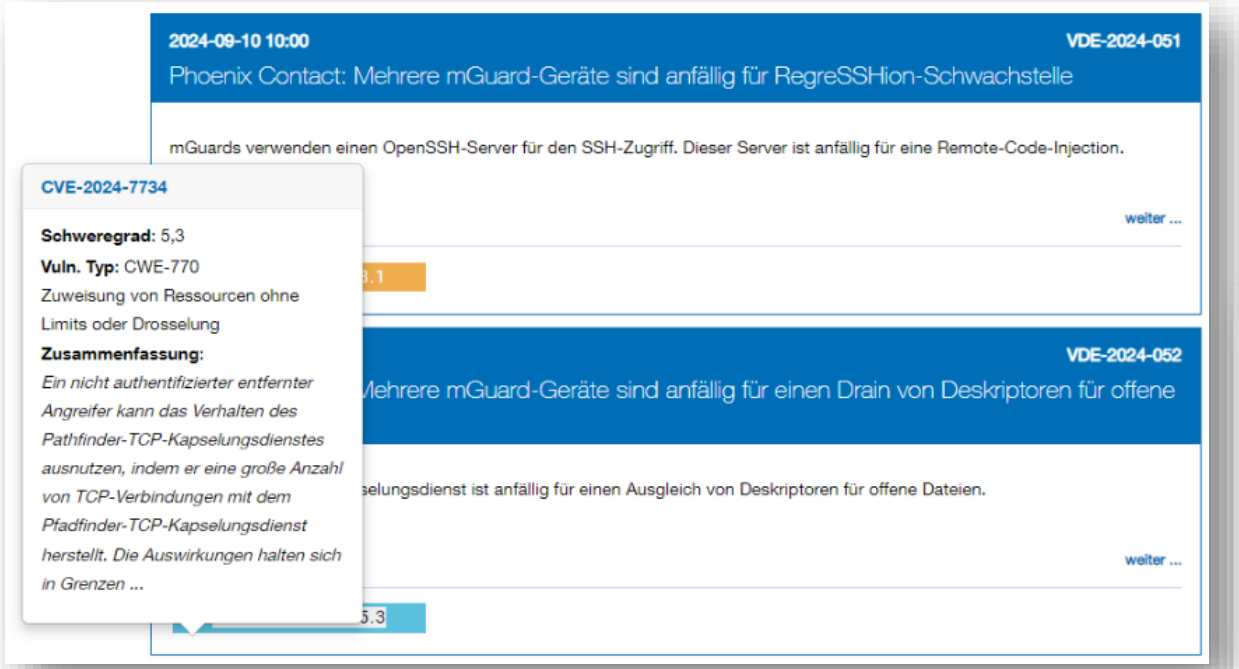
» Dokumentation der relevanten Cybersicherheitsaspekte des Produkts einschließlich der Schwachstellen

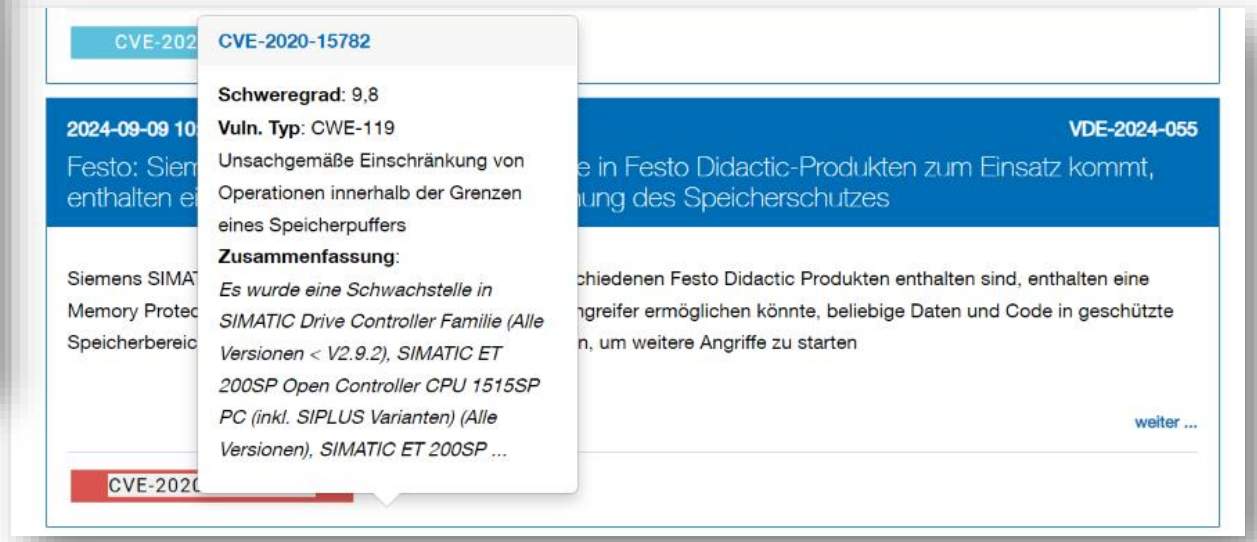
» Dokumentation für 10 Jahre nach dem Inverkehrbringen des Produkts oder für die Dauer des Supportzeitraums

» Schwachstellenbehandlung mindestens 5 Jahren, sofern die erwartbare Nutzungsdauer nicht kürzer ist

(CVE) (Bekannte Schwachstellen und Anfälligkeiten)

Ziel des CVE-Systems ist es, Mehrfachbenennungen derselben Gefahren durch verschiedene Unternehmen und Institutionen zu vermeiden. Eine bekannte Sicherheitslücke wird mit einer Nummer versehen, die aus dem Kürzel CVE, der Jahreszahl der Entdeckung des Problems sowie einer beliebigen fortlaufenden Nummer besteht (z. B. CVE-2020-1234). Dadurch wird eine eindeutige Identifizierung der Schwachstelle gewährleistet und ein reibungsloser Informationsaustausch zwischen den verschiedenen Datenbanken einzelner Hersteller ermöglicht.





VDE-2024-055 | CERT@VDE (certvde.com)

CRA - Anforderungen an digitale Produkte

Grundlegende Anforderungen nach Annex I Teil 1:

- In Verkehr bringen ohne bekannte Schwachstellen
- Sichere Standardeinstellungen (Auslieferungszustand)
- Bereitstellung von Sicherheitsupdates (5 Jahre)
- Design mit limitierter Angriffsfläche
- uvm.

Die „Software Bill of Materials“ (SBOM) ist eine verschachtelte Liste von Software-Komponenten, aus denen ein Software-System besteht. Mit dieser Inventarliste machen die Hersteller transparent, aus welchen eindeutig identifizierbaren Komponenten in welchen Versionen ihre Software-Produkte bestehen.

Schwachstellenmanagement Annex I Teil 2:

- Meldung, Behebung und Dokumentation von Schwachstellen
- Erstellung einer SBOM
- Regelmäßige Überprüfungen der Sicherheit
- Meldepflichtgegen über ENISA und CSIRT / PSIRT
- uvm.

Product Security Incident Response Team

ist bei Security-Incidents (Sicherheits-Vorfällen) die zentrale Anlaufstelle für Betreiber oder Integratoren von PRODUKTEN dieses Herstellers. Das Hersteller PSIRT analysiert, klassifiziert und bearbeitet gemeldete Schwachstellen und Incidents, von deren Produkten.

Das PSIRT informiert über bekannte Sicherheitsschwachstellen und bietet Updates oder Workaround zu den Security Advisories.

VDE CERT

CERT@VDE (certvde.com)

CERT@VDE (Verband der Elektrotechnik) ist die erste IT-Sicherheitsplattform in Deutschland für Unternehmen im Bereich der Automatisierung.

Mit der fortschreitenden Vernetzung von Produktionssystemen steigt auch das Risiko von Sicherheitslücken und dadurch von Angriffen auf Ihre Systeme.

adstec Industrial IT

auma Solutions for a world in motion

BECKHOFF New Automation Technology

BENDER The Power in Electrical Safety

CODESYS

DURAG GROUP TECHNOLOGY FOR A CLEAN AND SAFE ENVIRONMENT

Endress+Hauser People for Process Automation

FESTO

FRAUSCHER

CARLO GAVAZZI

Helmholz COMPATIBLE WITH YOU

HIMA SMART SAFETY.

ifm

K4 DIGITAL

Lenze

MB CONNECTLINE

Miele

PEPPERL+FUCHS

PHOENIX CONTACT

PILZ THE SPIRIT OF SAFETY

swarco

TRUMPF

VARTA

VEGA

WAGO

Weidmüller

W&T www.WuT.de

CRA - Meldepflichten der Hersteller

Meldung nach Kenntnis von jeder aktiv ausgenutzten Sicherheitslücke oder Vorfall an ENISA & CSIRT / PSIRT

1. Frühwarnmeldung innerhalb von 24h
2. Meldung mit Infos und ggf. Abhilfemaßnahmen innerhalb von 72h
3. Abschlussbericht von ausgenutzten Sicherheitslücken nach 14 Tagen; von Vorfällen nach 30 Tagen
   - Einschließlich Beschreibung, Schweregrad, Auswirkungen
   - Mögliche Ursachen und etwaige Akteure
   - Einzelheiten über Sicherheitsupdates & Abhilfemaßnahmen
4. Bereitstellung von Informationen über Risikominderung und Abhilfemaßnahmen an betroffene Nutzer

CRA - Sanktionen

- Nichteinhaltung der Anforderungen aus Annex I und der Verpflichtungen aus Art. 13 & Art. 14
- Geldbußen bis zu 15 Mio. € oder 2,5% des globalen Umsatzes, je nachdem, was höher ausfällt.
- Nichteinhaltung der Verpflichtungen aus den restlichen relevanten Artikeln
- Geldbußen bis zu 10 Mio. € oder 2% des globalen Umsatzes, je nachdem, was höher ausfällt.
- Erteilung falscher Auskünfte an notifizierende Stellen und Marktüberwachungsbehörden.
- Geldbußen bis zu 5 Mio. € oder 1% des globalen Umsatzes, je nachdem, was höher ausfällt.

Ausnahmen:

- Verwalter von Open Source Software (Insgesamt)
- Kleinst- und Kleinunternehmen (Meldefristen aus Art. 14)

CRA – Gültigkeit für den Handel

Hersteller und Importeure von „Produkten mit digitalen Elementen“ dürfen nach Inkrafttreten des CRA, Produkte ohne EU-Konformitätsnachweis (CE-Kennzeichnung) nach CRA-Richtlinie (2024/xxx/EU) nicht mehr in den Europäischen Markt einbringen.

Produkte, die den CRA nicht erfüllen, dürfen nur noch als Ersatzteile auf dem Markt bereitgestellt werden.

Produkten mit digitalen Elementen, die vom **Handel** vor dem Inkrafttreten des CRA (in den Markt eingebracht), als Lagerbestand gekauft wurden, können weiterhin verkauft werden.

Sollte der Importeur oder Produzent nicht auf die Einhaltung der entsprechenden Richtlinien achten, führt diese Zuwiderhandlung zu einem Bußgeld und zur Rücknahme der Waren vom Markt.

Verkaufen Händler Produkte ohne gültiger CE-Kennzeichnung kann dies einen Wettbewerbsverstoß darstellen und abgemahnt werden.