CONFIRMATE

CONFormIty assessment, metRics and compliance autoMATion for the cyber resiliencE act

Leitfaden zur Einhaltung des Cyber Resilience Act für KMU

Ausgabedatum: 30.10.2025
Status: final
Version: 1.0

Das im Rahmen der Finanzhilfevereinbarung **Nr. 101190193** finanzierte Projekt wird vom Europäischen Kompetenzzentrum für Cybersicherheit unterstützt. Die geäußerten Ansichten und Meinungen sind jedoch ausschließlich die der Autoren und spiegeln nicht unbedingt die der Europäischen Union oder des Europäischen Kompetenzzentrums für Cybersicherheit wider. Weder die Europäische Union noch die Bewilligungsbehörde können dafür haftbar gemacht werden.

Liste der Änderungen

Version	Datum	Beschreibung	Autor(en)
0.1	07.04.2025	Erster Entwurf	CYEN
0.2	27.06.2025	Zusätzlicher Text hinzugefügt	CYEN
0,3	06.08.2025	Erste Version fertiggestellt, zusätzlicher Text/zusätzliche Hinweise hinzugefügt	CYEN
0.4	03.09.2025	Version von den Projektpartnern geprüft, zur Verteilung an externe Peer-Review	CYEN
0.5	24.10.2025	Überarbeitete Version unter Berücksichtigung der Begutachtung	CYEN
1.0	30.10.2025	Endgültige veröffentlichte Fassung	CYEN

Mitwirkende

Rolle	Name des Mitwirkenden	Name der Einrichtung – Begünstigter
Verantwortlicher für die Lieferung	Iva Tasheva, Steve Purser, Krasimir Simonski, Azeez Kamal	CYEN
Mitwirkende	Christine Demeter, Gabriel Niculescu	DNSC
Mitwirkende	Andreas Binder	AISEC Fraunhofer
Peer Review	Harald Fischer	Balena
Peer Review	Argyro Chatzopoulou et al.	CURIUM-Projekt
Peer Review	Romain Muguet et al.	Red Alert Labs

Haftungsausschluss: Die Confirmate-Tools, einschließlich des CRA-Compliance-Leitfadens, dienen ausschließlich allgemeinen Informations- und Bildungszwecken. Sie bieten eine allgemeine Einführung in den CRA-Compliance-Prozess und sind nicht auf die Umstände einer bestimmten Organisation, eines bestimmten Produkts oder einer bestimmten Situation zugeschnitten. Der Inhalt spiegelt die individuellen Erfahrungen und Meinungen der beteiligten Experten, Autoren und Peer-Reviewer wider und ist möglicherweise nicht umfassend, wird nicht ständig aktualisiert oder ist nicht auf jeden Fall anwendbar.

Keine dieser Tools stellt eine rechtliche, regulatorische oder professionelle Beratung dar. Confirmate übernimmt keine Verantwortung oder Haftung für Maßnahmen, die auf der Grundlage der bereitgestellten Informationen ergriffen werden. Die Nutzer sind allein dafür verantwortlich, die Einhaltung der geltenden Gesetze, Vorschriften und Standards sicherzustellen.

Da sich die regulatorischen Anforderungen weiterentwickeln, empfehlen wir Ihnen dringend, einen qualifizierten Rechtsbeistand oder Regulierungsexperten zu konsultieren, um eine auf Ihre Situation zugeschnittene Beratung zu erhalten.

Inhalt

1. Glossar: Akronyme, Begriffe und Abkürzungen

Die folgenden Begriffe kommen im Text dieser Leitlinien vor:

Bevollmächtigter Vertreter:	Eine in der Union ansässige natürliche oder juristische Person, die von einem Hersteller schriftlich beauftragt wurde, in seinem Namen bestimmte Aufgaben wahrzunehmen.
CE-Kennzeichnung:	Kennzeichnung, mit der ein Hersteller angibt, dass ein Produkt mit digitalen Elementen und die vom Hersteller eingerichteten Prozesse den grundlegenden Cybersicherheitsanforderungen gemäß Anhang I der CRA und anderen geltenden Harmonisierungsrechtsvorschriften der Union entsprechen, die seine Anbringung vorschreiben.
Konformitätserklärung (DoC):	Ein vom Hersteller erstelltes Rechtsdokument, in dem bestätigt wird, dass ein Produkt die geltenden grundlegenden Anforderungen der CRA erfüllt. Es muss den zuständigen Behörden sowie den Nutzern als Teil der technischen Dokumentation zur Verfügung gestellt werden.
Konformitätsbewertung:	Prozess der Überprüfung, ob die in Anhang I der CRA festgelegten grundlegenden Cybersicherheitsanforderungen erfüllt sind.
Harmonisierte Norm:	Eine technische Spezifikation, die von einer europäischen Normungsorganisation (ESO) auf Ersuchen der Europäischen Kommission entwickelt wurde, um die Umsetzung der europäischen Rechtsvorschriften zu unterstützen. Dabei handelt es sich um offiziell anerkannte europäische Normen, die die Konformität mit bestimmten rechtlichen Anforderungen der EU-Rechtsvorschriften vermuten lassen.
Vorfall:	Ereignis, das die Fähigkeit eines Produkts mit digitalen Elementen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder Funktionen zu schützen, beeinträchtigt oder beeinträchtigen kann.
Vertreiber:	Eine natürliche oder juristische Person in der Lieferkette, mit Ausnahme des Herstellers oder Einführers, die ein Produkt mit digitalen Elementen auf dem Unionsmarkt bereitstellt, ohne dessen Eigenschaften zu beeinflussen.
Einführer:	Eine in der Union ansässige natürliche oder juristische Person, die ein Produkt mit digitalen Elementen in Verkehr bringt, das den Namen oder die Marke eines außerhalb der Union ansässigen Herstellers trägt.
Hersteller:	Eine natürliche oder juristische Person, die Produkte mit digitalen Elementen entwickelt oder herstellt oder Produkte mit digitalen Elementen entwerfen, entwickeln oder herstellen lässt und diese unter ihrem Namen oder ihrer Marke gegen Entgelt, zur Monetarisierung oder kostenlos in Verkehr bringt.
New Legislative Framework (NLF):	Vorschriften, die strukturierte und harmonisierte Anforderungen für die Bewertung der Produktkonformität vor dem Inverkehrbringen von Waren auf dem EU-Markt festlegen.
Produkt mit digitalen Elementen (PDE):	Ein Software- oder Hardwareprodukt und seine Lösungen zur Fernverarbeitung von Daten, einschließlich Software- oder Hardwarekomponenten, die separat in Verkehr gebracht werden.
KMU:	Die Kategorie der kleinen und mittleren Unternehmen (KMU) umfasst Unternehmen, die weniger als 250 Personen beschäftigen und einen Jahresumsatz

	von höchstens 50 Millionen Euro und/oder eine Jahresbilanzsumme von höchstens 43 Millionen Euro haben. Innerhalb der KMU-Kategorie wird ein kleines Unternehmen als ein Unternehmen definiert, das weniger als 50 Personen beschäftigt und dessen Jahresumsatz und/oder Jahresbilanzsumme 10 Millionen Euro nicht übersteigt, während für ein Kleinstunternehmen diese Schwellenwerte bei weniger als 10 Beschäftigten und weniger als 2 Millionen Euro liegen.
Software-Stückliste:	Eine formelle Aufzeichnung mit Details und Lieferkettenbeziehungen der Komponenten, die in den Softwareelementen eines Produkts mit digitalen Elementen enthalten sind.
Supportzeitraum:	Der Zeitraum, in dem ein Hersteller sicherstellen muss, dass Schwachstellen eines Produkts mit digitalen Elementen wirksam und in Übereinstimmung mit den wesentlichen Cybersicherheitsanforderungen gemäß Anhang I Teil II der CRA behandelt werden.
Sicherheitslücke:	Schwäche, Anfälligkeit oder Fehler eines Produkts mit digitalen Elementen, die von einer Cyber-Bedrohung ausgenutzt werden können. - Eine ausnutzbare Schwachstelle ist eine Schwachstelle, die von einem Angreifer unter praktischen Betriebsbedingungen effektiv genutzt werden kann. - Eine aktiv ausgenutzte Schwachstelle ist eine Schwachstelle, für die es zuverlässige Hinweise darauf gibt, dass ein böswilliger Akteur sie in einem System ohne Erlaubnis des Systembesitzers ausgenutzt hat.

2. Einleitung

Über das Confirmate-Projekt

CONFIRMATE ist ein innovatives Projekt, das von der Europäischen Union (EU) und dem European Cybersecurity Competence Centre and Network (ECCC) kofinanziert wird und kleinen und mittleren Unternehmen im Fertigungsbereich dabei helfen soll, den sich ständig weiterentwickelnden Cybersicherheitsvorschriften einen Schritt voraus zu sein. Zur Vereinfachung der Einhaltung des EU-Cyberresilienzgesetzes (CRA) bietet CONFIRMATE Open-Source-Tools, praktische Schulungen und standardisierte Methoden, die die Einhaltung des CRA zugänglicher, effizienter und kostengünstiger machen.

Der Name des Projekts steht für „Conformity Assessment, Metrics, and Automation for the Cyber Resilience Act" (Konformitätsbewertung, Metriken und Automatisierung für das Gesetz zur Cyber-Resilienz). Auf der Grundlage des Open-Source-Frameworks Clouditor bietet CONFIRMATE automatisierte Service-Zerlegung und Compliance-Ansichten, klare Bewertungsergebnisse, eine robuste Penetrationstest-Methodik, mehrsprachige Cybersicherheitsschulungsmodule[1] und einen umfassenden CRA-Compliance-Leitfaden (dieses Dokument). Siehe veröffentlichte Materialien in Anhang E.

CONFIRMATE bringt führende Partner wie CYEN, Fraunhofer AISEC, ITKAM und die rumänische Nationale Direktion für Cybersicherheit (DNSC) zusammen und stattet KMU mit dem Wissen und den Ressourcen aus, die sie benötigen, um wichtige Cybersicherheitsanforderungen sicher zu erfüllen und die Widerstandsfähigkeit ihrer digitalen Produkte zu gewährleisten. Weitere derzeit laufende EU-Projekte und die Einhaltung der CRA durch KMU sind in Anhang F aufgeführt.

2.1 Zweck und Zielgruppe dieses Leitfadens

Dieser Compliance-Leitfaden ist eine kostenlose Ressource, die KMU im verarbeitenden Gewerbe in der EU dabei unterstützen soll, die wesentlichen Cybersicherheitsanforderungen des EU-Cyberresilienzgesetzes (CRA)[2] zu verstehen. Der Leitfaden wurde speziell entwickelt, um einen Überblick über die Compliance-Anforderungen zu geben und KMU dabei zu unterstützen, die Erwartungen in umsetzbare, leicht verständliche Schritte zu unterteilen. Er ist auf die besonderen Bedürfnisse und Herausforderungen von KMU im verarbeitenden Gewerbe zugeschnitten. Der ursprünglich in englischer Sprache verfasste Leitfaden wird in vier europäische Sprachen übersetzt: Deutsch, Französisch, Italienisch und Rumänisch, wodurch über 60 % der EU-Bevölkerung erreicht werden können.

[1] Siehe Einführungsvideo auf YouTube: https://youtu.be/QeIjDeVvbL0
[2] Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

Der Leitfaden bietet einen umfassenden Überblick über das EU-Gesetz zur Cyberresilienz (CRA) und behandelt wichtige Aspekte wie Rollen und Verantwortlichkeiten, wesentliche Cybersicherheitsanforderungen, Konformitätsbewertungsverfahren und die Meldung von Vorfällen mit Verpflichtungen nach dem Inverkehrbringen. Er enthält außerdem praktische Schritte für KMU zur Umsetzung des CRA sowie Vorschläge für unterstützende Tools, Vorlagen und Ressourcen zur Verbesserung ihrer Sicherheitslage und zur Unterstützung einer kontinuierlichen Verbesserung.

Zweck: Der Hauptzweck des Leitfadens besteht darin, KMU zu stärken, indem ihnen das notwendige Wissen und die erforderlichen Instrumente zur Verfügung gestellt werden, um die Einhaltung des CRA zu erreichen und aufrechtzuerhalten. Er zielt darauf ab, die Komplexität der regulatorischen Anforderungen zu verringern, damit Unternehmen ihre Verpflichtungen sicher erfüllen und sich gleichzeitig auf ihr Kerngeschäft konzentrieren können. Darüber hinaus dient der Leitfaden dazu, KMU die Bedeutung des Managements von Cybersicherheitsrisiken, des Schutzes ihres Rufs und der Gewährleistung der Sicherheit und Vertrauenswürdigkeit ihrer digitalen Produkte vor Augen zu führen. Letztendlich soll er KMU mit dem Wissen und den praktischen Schritten ausstatten, um die Cyber-Resilienz ihrer Produkte zu verbessern.

Zielgruppe: Der Leitfaden ist speziell auf europäische KMU zugeschnitten, die Produkte mit digitalen Elementen entwickeln, herstellen oder vermarkten. Diesen Unternehmen fehlen oft die umfangreichen Ressourcen und das Fachwissen größerer Organisationen, sodass die Einhaltung komplexer Vorschriften wie der CRA eine erhebliche Herausforderung darstellt. Durch die Fokussierung auf KMU versucht der Leitfaden, deren spezifische Herausforderungen anzugehen, wie z. B. begrenzte Budgets, kleinere Teams und der Bedarf an praktischen, skalierbaren Lösungen.

Trotz des Verständnisses für die oben genannten Herausforderungen, denen KMU gegenüberstehen, gelten die CRA-Verpflichtungen für KMU mit wenigen Ausnahmen, d. h. vereinfachte Dokumentationsvorlagen (technische Dokumentation und Konformitätserklärung) und vorrangige Leitlinien, die auch in diesem Leitfaden behandelt werden, genauso wie für große Unternehmen.

In diesem Sinne gelten alle Leitlinien in diesem Dokument, sofern nicht ausdrücklich anders angegeben, für KMU.

Dieser Compliance-Leitfaden ist also eine wertvolle Ressource für KMU im verarbeitenden Gewerbe in der EU, da er Klarheit, Sicherheit und praktische Instrumente bietet, um die Anforderungen des EU-Cyberresilienzgesetzes zu erfüllen. Er unterstützt nicht nur die Einhaltung der Vorschriften, sondern fördert auch eine Kultur der Cybersicherheit und hilft KMU, ihre Produkte, Kunden und ihren Ruf in einem zunehmend digitalisierten Markt zu schützen.

2.2 Wichtige Fragen und Antworten zum Cyber Resilience Act (CRA)

Frage 1: Was ist der Cyber Resilience Act (CRA)?
Der CRA ist eine EU-Verordnung, die darauf abzielt, die Cybersicherheit von Produkten mit digitalen Elementen (PDEs) wie vernetzten Geräten und Software zu gewährleisten. Er führt verbindliche Sicherheitsanforderungen für den gesamten Produktlebenszyklus ein, vom Design bis zum Kundendienst nach dem Verkauf.

Obwohl weithin anerkannt, sollte die Definition des CRA für Produkte mit digitalen Elementen (PDE) näher erläutert werden, da sie sich darauf bezieht, ob Produkte von KMU die Anforderungen erfüllen müssen.

Per Definition umfasst PDE Software- oder Hardwareprodukte und deren Lösungen zur Fernverarbeitung von Daten. Bei Software gibt es hier keinen Interpretationsspielraum, da sie leicht als Programmcode zu erkennen ist. Bei Hardware hingegen muss klargestellt werden, dass sie in der Lage sein muss, digitale Daten zu verarbeiten, zu speichern oder zu übertragen und separat auf den Markt gebracht werden kann, selbst wenn sie als Bestandteil eines anderen Produkts Teil einer Lieferkette ist.

Frage 2: Gilt der CRA für unsere Produkte?
Wenn Ihr Unternehmen Produkte mit digitalen Elementen herstellt oder auf dem EU-Markt vertreibt (z. B. IoT-Geräte, eingebettete Software, Industriemaschinen mit Netzwerkschnittstellen), dann ja, der CRA gilt wahrscheinlich. Ausnahmen gelten für bereits regulierte Produkte wie Medizinprodukte, Leichtfahrzeuge, Luftfahrt, Produkte, die ausschließlich für militärische Zwecke, nationale Sicherheit und die Verwendung geheimer Informationen bestimmt sind.

Frage 3: Bin ich vom CRA betroffen?
Wenn Sie Hersteller, Einführer, Händler und Open-Source-Verwalter eines auf dem EU-Markt platzierten PDE sind, haben Sie bestimmte Verpflichtungen gemäß des CRA.

Frage 4: Was sind die wichtigsten Verpflichtungen für Hersteller?

- Durchführung und Dokumentation **von Cybersicherheits-Risikobewertungen,** einschließlich Risiken in der Lieferkette
- Sicherstellung von **„Secure-by-Design"-** und **„Secure-by-Default**"-Praktiken
- Implementierung von Prozessen **zum Umgang mit Schwachstellen**, einschließlich der Meldung und Nulltoleranz für aktiv ausgenutzte Schwachstellen, die der Öffentlichkeit bekannt sind.
- Bereitstellung von **Sicherheitsupdates** für den Produktlebenszyklus
- **Durchführung von Konformitätsbewertungsverfahren, die** an die Produktklasse angepasst sind
- Erstellung und Pflege von **technischer Dokumentation, Benutzerinformationsdateien, EU-Konformitätserklärung** (in den Sprachen des Marktlandes)

F5. Wann tritt der CRA in Kraft?

Der CRA wird schrittweise umgesetzt. Wichtige Termine für Hersteller sind:

- ➔ **11. September 2026,** wenn die Meldepflichten für Schwachstellen und Sicherheitsvorfälle in Kraft treten.
- ➔ **11. Dezember 2027,** wenn der CRA vollständig in Kraft tritt.

Frage 6: Welche Strafen drohen bei Nichteinhaltung?
Die Nichteinhaltung kann zu Geldstrafen von bis zu **15 Millionen Euro oder 2,5 % des weltweiten Jahresumsatzes** führen, je nachdem, welcher Betrag höher ist. Auch der Rückzug vom Markt und Reputationsschäden sind Risiken.

Frage 7: Was sollten Hersteller jetzt tun?

- **Erstellen Sie eine Übersicht über Ihr Produktportfolio** hinsichtlich der Anwendbarkeit des CRA.
- Beginnen Sie mit **Cybersicherheits-Risikobewertungen und Lückenanalysen.**
- Aktualisieren Sie **das Design, die technische Dokumentation und die Support-Richtlinien.**
- **Erwägen Sie die Anpassung an Cybersicherheitsstandards** (z. B. EUCC, ISO/IEC 2700x, ETSI EN 303 645).

2.3 Hintergrund und Zielsetzung des Cyber Resilience Act (CRA)

Der Cyber Resilience Act ist eine Fortsetzung der ersten horizontalen Produktsicherheitsvorschrift, der Funkgeräterichtlinie (RED)[3], die die ersten Cybersicherheitsanforderungen für eine breite Palette von in der EU verkauften Produkten eingeführt hat, insbesondere für mit dem Internet verbundene Geräte und solche, die personenbezogene Daten verarbeiten. Diese Anforderungen sind seit dem 1. August 2025 verbindlich. Diese in Artikel 3 Absatz 3 der RED dargelegten Anforderungen zielen darauf ab, die Sicherheit von Nutzern und Netzwerken zu verbessern, indem sie sich mit Netzwerkschutz, Datenschutz und Betrugsbekämpfung befassen. Der CRA steht auch im Zusammenhang mit der Produkthaftungsrichtlinie (PLD),[4] die sich mit der Haftung für fehlerhafte Produkte, einschließlich solcher mit digitalen Elementen, befasst.

Die Ziele des EU-Cyberresilienzgesetzes (CRA) bestehen darin, *„die Cybersicherheitsstandards von Produkten [zu verbessern], die eine digitale Komponente enthalten, und Hersteller und Einzelhändler [zu verpflichten], die Cybersicherheit während des gesamten Lebenszyklus ihrer Produkte sicherzustellen. (...) Das Cyber Resilience Act befasst sich mit dem unzureichenden Cybersicherheitsniveau in vielen Produkten und dem Mangel an rechtzeitigen Sicherheitsupdates für Produkte und Software“*.[5] Der CRA zielt darauf ab, ein einheitliches und hohes Maß an Cybersicherheit zu schaffen, indem klare Anforderungen an Hersteller,

[3] Richtlinie 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0053
[4] Richtlinie (EU) 2024/2853 des Europäischen Parlaments und des Rates vom 23. Oktober 2024: https://eur-lex.europa.eu/eli/dir/2024/2853/oj/eng
[5] Europäische Kommission (2025) Cyber-Resilienz-Gesetz, abgerufen am 14. April 2025 hier: https://digital-strategy.ec.europa.eu/de/policies/cyber-resilience-act

Entwickler, Einführer und Händler gestellt werden und gleichzeitig die Transparenz in Bezug auf Cybersicherheitsrisiken gefördert wird.

Laut EU-Kommission wir mit dem CRA „*folgendes sichergestellt:*

- *Drahtgebundene und drahtlose mit dem Internet verbundene Produkte und Software, die in der EU in Verkehr gebracht werden, werden sicherer;*
- *die Hersteller bleiben während des gesamten Lebenszyklus eines Produkts für seine Cybersicherheit verantwortlich;*
- *die Verbraucherinnen und Verbraucher werden angemessen über die Cybersicherheit der Produkte, die sie kaufen und verwenden, informiert.*

[…] Es verpflichtet die Hersteller, die Cybersicherheit bei der Konzeption und Entwicklung von Produkten mit digitalen Elementen zu berücksichtigen“.[6]

Diese Verpflichtungen müssen in jeder Phase der Wertschöpfungskette erfüllt werden. Der CRA betont die Grundsätze der Sicherheit durch Design, Konformitätsbewertungen und die Meldung von Cybervorfällen und aktiv ausgenutzten Schwachstellen, um ein sichereres digitales Ökosystem zu schaffen.

Die Auswirkungen des CRA beschränken sich nicht auf einen bestimmten Sektor, sondern ermöglichen eine breitere Wirkung und legen ein Mindestmaß an akzeptabler Sicherheit für Produkte fest, die in der gesamten EU verkauft werden. Damit trägt er zu einer besseren Cyber-Resilienz bei. Insbesondere für KMU bietet der CRA einen Rahmen für die Integration der Cybersicherheit in ihre Prozesse und hilft ihnen so, auf einem sicheren und vertrauenswürdigen Markt zu bestehen.

Der Zusammenhang und die Beziehung zwischen der CRA und anderen relevanten EU-Sicherheitsvorschriften werden in Anhang G „Bezug zu anderen EU-Rechtsvorschriften“ dieses Dokuments beschrieben.

2.4 Geltungsbereich und Durchsetzung des Cyber-Resilienz-Gesetzes (CRA)

Geltungsbereich: Die CRA gilt für alle Produkte mit digitalen Elementen, die auf dem EU-Markt in Verkehr gebracht werden (d. h. separat verkauft werden und nicht Teil einer Dienstleistung sind) *und „direkt oder indirekt mit einem anderen Gerät oder Netzwerk verbunden sind, mit Ausnahme bestimmter Ausnahmen wie bestimmte quelloffene Software- oder Dienstleistungsprodukte, die bereits unter bestehende Vorschriften fallen, was für Medizinprodukte, Luftfahrt und Autos der Fall ist. Produkte tragen die CE-Kennzeichnung, um anzuzeigen, dass sie die CRA-Anforderungen erfüllen“.*[7] Die Verpflichtungen erstrecken sich über den gesamten Lebenszyklus des Produkts, von der Konzeption über die Entwicklung, Produktion und Wartung bis hin zur Entsorgung.

[6] Europäische Kommission (2025) Cyber-Resilienz-Gesetz, abgerufen am 14. April 2025 hier: https://ec.europa.eu/commission/presscorner/detail/de/qanda_22_5375
[7] Europäische Kommission (2025) Cyber-Resilienz-Gesetz, abgerufen am 14. April 2025 hier: https://digital-strategy.ec.europa.eu/de/policies/cyber-resilience-act

Es sei darauf hingewiesen, dass ein PDE, das nicht direkt mit einem Netzwerk oder einem anderen elektronischen Informationssystem verbunden ist, dennoch indirekt eine Bedrohung für ein bestimmtes Ziel durch infizierte Dateien, Flash-Laufwerke usw. darstellen kann (Erwägungsgrund 9). Dabei kann es sich um ein eigenständiges Gerät wie ein Smart Lock, ein Spielzeug oder ähnliches handeln (Erwägungsgrund 10).

„Auf der Grundlage des neuen EU-Rechtsrahmens für Produktvorschriften *würden die Hersteller einem Konformitätsbewertungsverfahren unterzogen, um nachzuweisen, dass die für ein Produkt festgelegten Anforderungen eingehalten wurden.*

Dies könnte je nach dem Risikoniveau des betreffenden Produkts durch eine Selbstbewertung oder eine Konformitätsbewertung durch Dritte erfolgen".[8]

Der CRA klassifiziert Produkte mit digitalen Elementen in vier Kategorien (Standard, wichtig Klasse I, wichtig Klasse II, kritisch). Alle Produktkategorien müssen die gleichen grundlegenden Cybersicherheitsanforderungen erfüllen (die im Gesetz festgelegt sind und in Abschnitt 3 dieses Dokuments erläutert werden), aber je nach Risiko und Notwendigkeit unterschiedliche Durchsetzungsmaßnahmen (Konformitätsbewertungsverfahren) befolgen:

- **Standardprodukte mit digitalen Elementen** machen etwa 90 % aller Produkte mit digitalen Elementen aus. Sie müssen grundlegende Cybersicherheitsanforderungen erfüllen und dies durch Selbstbewertung und Konformitätserklärung bestätigen.
- **Wichtige Produkte mit digitalen Elementen** sind in Anhang III aufgeführt und in zwei Kategorien unterteilt – Klasse I und Klasse II**.** Diese Produkte erfüllen Funktionen, die für die Cybersicherheit anderer Produkte, Netzwerke oder Dienste von entscheidender Bedeutung sind, und stellen in diesem Sinne ein erhebliches Risiko dar. Zusätzlich zur Erfüllung der grundlegenden Cybersicherheitsanforderungen gelten für sie strengere Anforderungen an die Cybersicherheitsprüfung, bevor sie in Verkehr gebracht werden dürfen.
- **Kritische Produkte mit digitalen Elementen** sind in Anhang IV aufgeführt. Es handelt sich um eine sehr begrenzte Liste von Produkten, die als besonders risikoreich gelten und für die gemäß einer gemäß der Verordnung (EU) 2019/881 angenommenen europäischen Cybersicherheitszertifizierungsregelung ein europäisches Cybersicherheitszertifikat mit einem Sicherheitsniveau von mindestens „erheblich" erforderlich ist.

[8] Europäische Kommission (2025) Cyber-Resilienz-Gesetz, abgerufen am 14. April 2025 hier: https://ec.europa.eu/commission/presscorner/detail/de/qanda_22_5375

3. Rollen und Verantwortlichkeiten

Die CRA-Verpflichtungen richten sich an eine Vielzahl von Akteuren in der Lieferkette eines Produkts, ohne Unterscheidung nach Größe oder Herkunft, sondern mit Fokus auf der Rolle der juristischen oder natürlichen Person in Bezug auf das betreffende PDE. Es werden jedoch Leitlinien (wie in diesem Dokument dargelegt) und vereinfachte Vorlagen veröffentlicht, damit insbesondere KMU ihre Aufgaben und Verantwortlichkeiten so effektiv und effizient wie möglich erfüllen können.

Der CRA definiert spezifische Rollen und entsprechende Verantwortlichkeiten wie folgt:

3.1 Hersteller

Hersteller spielen eine wichtige Rolle für die Cybersicherheit von Produkten mit digitalen Elementen in der Entwurfs-, Entwicklungs-, Produktions- und Supportphase. Als solcher ist der Hersteller das führende Unternehmensprofil in der CRA und trägt die gesamte Verantwortung (d. h. die Umsetzung der wesentlichen Cybersicherheitsanforderungen und Konformitätsbewertungsverfahren).

Der CRA definiert einen Hersteller als *„eine natürliche oder juristische Person, die Produkte mit digitalen Elementen entwickelt oder herstellt oder die Produkte mit digitalen Elementen konzipieren, entwickeln oder herstellen lässt und sie unter ihrem Namen oder ihrer Marke vermarktet, sei es gegen Bezahlung, zur Monetarisierung oder unentgeltlich*“.

Diese Definition impliziert, dass alle Phasen des Produktlebenszyklus von einem einzigen Hersteller durchgeführt werden, der die gesamte Verantwortung für die Cybersicherheit des Produkts trägt. In der Praxis ist die Produktionskette bekanntlich viel komplexer und umfasst Lieferketten, Dritte und andere Akteure, was jedoch nicht zu einer geteilten Verantwortung führt.

Für jede Phase des Produktlebenszyklus gibt es spezifische Cybersicherheitsanforderungen für jede einzelne Aktivität, Phase und Operation. Die Verantwortlichkeiten des Herstellers enden nicht einmal mit dem Inverkehrbringen des PDE.

Die Pflichten der Hersteller (siehe Tabelle 1) sind in den Artikeln 13 und 14 des CRA im offiziellen Text zusammengefasst und werden im vorliegenden Dokument erläutert.

Verpflichtung	Tätigkeit
Umsetzung der grundlegenden Cybersicherheitsanforderungen der CRA	Bei der Inverkehrbringung eines Produkts mit digitalen Elementen müssen Hersteller sicherstellen, dass es gemäß den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I entwickelt und hergestellt wurde. gemäß den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I entworfen, entwickelt und hergestellt wurde.
Regelmäßige Risikobewertung	Durchführung und regelmäßige Aktualisierung von Cybersicherheitsrisikobewertungen für Produkte und die Lieferkette. Berücksichtigung der Bewertungsergebnisse bei der Planung, Konzeption, Entwicklung, Herstellung, Lieferung und Wartung von PDEs, um Cybersicherheitsrisiken zu minimieren, Vorfälle zu verhindern und deren Auswirkungen zu minimieren, auch in Bezug auf die Gesundheit und Sicherheit der Nutzer. Die Cybersicherheitsrisikobewertung muss angeben, wie die grundlegenden Cybersicherheitsanforderungen (einschließlich Umgang mit Schwachstellen) umgesetzt werden.
Sicherheit durch Design und Standardeinstellungen	Sicherstellung, dass Produkte sicher konzipiert sind und mit sicheren Standardkonfigurationen geliefert werden.
Schwachstellenmanagement	Implementierung klarer Prozesse mit Nulltoleranz für öffentlich bekannte, aktiv ausgenutzte Schwachstellen.
Sicherheitsupdates	Bereitstellung von zeitnahen, kostenlose Sicherheitsupdates, die von Funktionsupdates getrennt sind, während des gesamten Produktlebenszyklus.
Konformität und CE-Kennzeichnung	Durchführung einer Konformitätsbewertung (Selbstbewertung oder durch Dritte) und Anbringung von CE-Kennzeichnung.
Dokumentation und DoC	Erstellung und Pflege der technischen Dokumentationen und der EU-Konformitätserklärung (in den Sprachen des Zielmarktes).
Berichterstattung	Meldung aktiv ausgenutzter Schwachstellen und bedeutender Vorfälle mit Auswirkungen auf die Sicherheit wie folgt gleichzeitig an CSIRT und ENISA über die einheitliche (EU-)Meldeplattform:
	- Frühwarnung: innerhalb von 24 Stunden
	- Erstmeldung: innerhalb von 72 Stunden
	- Abschlussbericht: innerhalb von 14 Tagen (Sicherheitslücke) / 1 Monat (Vorfall)
	Informieren der betroffenen Nutzenden des Produkts mit digitalen Elementen

Tabelle 1: Die Pflichten der Hersteller

In Abschnitt 3 dieses Dokuments werden die wesentlichen Cybersicherheitsanforderungen im Anhang I des Gesetzes detailliert beschrieben. Hier sind sie kurz zusammengefasst:

- Durchführung und Dokumentation einer Bewertung der Cybersicherheitsrisiken, einschließlich der Risiken in der Lieferkette
- Sicherstellung von „Secure-by-Design"- und „Secure-by-Default"-Praktiken
- Implementierung von Verfahren zum Umgang mit Schwachstellen, einschließlich der Meldung und Nulltoleranz für aktiv ausgenutzte Schwachstellen, die der Öffentlichkeit bekannt sind
- Bereitstellung von Sicherheitsupdates für den Produktlebenszyklus
- Durchführung von Konformitätsbewertungsverfahren, die an die Produktklasse angepasst sind
- Erstellung und Pflege von technischer Dokumentation, Benutzerinformationsdateien, EU-Konformitätserklärung (in den Sprachen des Landes, in dem das Produkt in Verkehr gebracht wird, einschließlich der erforderlichen Informationen. Eine vereinfachte Vorlage für die Konformitätserklärung für KMU findet sich in Anhang VI des CRA und Anhang I des vorliegenden Dokuments)

KMU, die als Hersteller anerkannt sind, sollten beachten, dass der CRA eine Meldepflicht für aktiv ausgenutzte Schwachstellen und schwerwiegende Vorfälle vorsieht, sobald der Hersteller davon Kenntnis erlangt hat. Ein Vorfall gilt als schwerwiegend, wenn er durch bösartigen Code verursacht wird oder diesen einführen kann oder wenn er die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit sensibler oder wichtiger Daten oder Funktionen des PDE beeinträchtigt.

Obwohl Kleinst- und Kleinunternehmen keine Verwaltungsstrafen zu befürchten haben, wenn sie die Frühwarnfrist von 24 Stunden nicht einhalten, wird ihnen empfohlen, dies so schnell wie möglich zu tun. Die Meldepflichten werden in Kapitel 6 ausführlich behandelt.

3.2 Verwalter quelloffener Software

Die Rolle des Verwalters quelloffener Software ist für KMU sehr typisch, da das Konzept des freien und quelloffenen Codes aus der KMU- und Freiberufler-Gesellschaft stammt und eher gemeinschaftsorientiert als kommerziell ist. Daher ist die Einführung von Verpflichtungen für Open-Source-Softwareanbieter schwierig zu definieren, wenn sie Teil der Lieferkette für die Herstellung von Produkten mit digitalen Elementen sind.

Die Definition des Verwalters quelloffener Software qualifiziert ihre PDE als freie und quelloffene Software, wobei erwartet wird, dass sie systematisch und nachhaltig unterstützt wird, und dass sie für kommerzielle Aktivitäten bestimmt ist.
Anbieter von Open-Source-Software werden von der CRA nicht als Hersteller eingestuft, es sei denn, sie üben kommerzielle Aktivitäten mit Open-Source-Software aus, wie z. B. die

Berechnung von Gebühren für die Software selbst, die Bereitstellung von technischem Support gegen Entgelt oder die Monetarisierung durch damit verbundene Dienstleistungen. Dies wird in Erwägungsgrund 18 der CRA klar zum Ausdruck gebracht: „nur freie und quelloffene Software, die auf dem Markt bereitgestellt und somit zum Vertrieb oder zur Nutzung im Rahmen einer Geschäftstätigkeit verfügbar gemacht wird, [sollte] in den Anwendungsbereich dieser Verordnung fallen."

Obwohl die CRA keine Verwaltungsstrafen für Open-Source-Software-Verwalter festlegt, unterliegen diese einem leichtgewichtigen Regulierungssystem mit Verpflichtungen, die in Artikel 24 der CRA aufgeführt und in Tabelle 2 unten zusammengefasst sind.

Verpflichtung	Aktivität
Richtlinie zur Cybersicherheit und zum Umgang mit Schwachstellen	Einführung und Dokumentation einer Cybersicherheitsrichtlinie zur Förderung der Entwicklung einer sicheren PDE sowie eines wirksamen Umgangs mit Schwachstellen durch die Entwickler dieses Produkts, wobei die freiwillige Meldung von Schwachstellen und der Austausch von Informationen über entdeckte Schwachstellen innerhalb der Open-Source-Community gefördert werden.
Zusammenarbeit	Auf Anfrage mit den Marktüberwachungsbehörden zusammenarbeiten, um die Cybersicherheitsrisiken von freien und Open-Source-Softwareprodukten zu mindern.
Benachrichtigung	Benachrichtigen der zuständigen Behörden und betroffenen Nutzer (oder aller Nutzer) über aktiv ausgenutzte Schwachstellen (sofern Sie an der Entwicklung des Produkts beteiligt sind) und schwerwiegende Vorfälle, die sich auf die Sicherheit von Produkten mit digitalen Elementen und auf Netz- und Informationssysteme auswirken, die von den Verwaltern quelloffener Software für die Entwicklung solcher Produkte bereitgestellt werden.
	Gebenenfalls Mitteilung aller Risikominderungs- und Korrekturmaßnahmen, die die Nutzer ergreifen können, um die Auswirkungen dieser Schwachstelle oder dieses Vorfalls zu mindern.

Tabelle 2: Die Pflichten von Verwaltern quelloffener Software

Die Artikel 21 und 22 des CRA behandeln Fälle, in denen die Verpflichtungen der Hersteller für andere Parteien gelten. Diese Leitlinien sind daher auch in diesen Fällen relevant.

3.3 Einführere und Händler

KMU können auch Einführer oder Händler von Produkten mit digitalen Elementen sein. Für diese Rollen legt die CRA in den Artikeln 19 und 20 jeweils spezifische Verpflichtungen fest, wie z. B. die Einhaltung der in Kapitel 3 unten behandelten grundlegenden Cybersicherheitsanforderungen und die Übernahme einiger der Herstellerpflichten.

Ein Einführer ist definiert als *„eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die ein Produkt mit digitalen Elementen unter dem Namen oder der Marke einer außerhalb der Union ansässigen oder niedergelassenen natürlichen oder juristischen Person in der Union in den Verkehr bringt".*

Ein Händler hingegen ist *„eine natürliche oder juristische Person in der Lieferkette, die ein Produkt mit digitalen Elementen ohne Änderung seiner Eigenschaften auf dem Unionsmarkt bereitstellt".*

Diese Leitlinien wurden zwar mit Blick auf Hersteller erstellt, können aber sinnvollerweise sowohl von Einführern als auch von Händlern verwendet werden, sofern die Unterschiede in den für diese Gruppen geltenden Verpflichtungen verstanden werden.

Die wichtigsten Verpflichtungen für Einführere (Artikel 19) und Händler (Artikel 20) sind in Tabelle 3 unten zusammengefasst:

Verpflichtung	Tätigkeit	Akteur	
		Importeur	Händler
Nur CRA-konforme Produkte auf den EU-Markt bringen	Keine Produkte auf den EU-Markt bringen, die nicht CRA-konform sind	✅	✅
Behandeln Sie nicht konforme Produkte	Sorgen für Korrekturen oder Rückzug/-ruf von Produkten bei Verdacht auf nicht-Konformität mit dem CRA oder dessen Anhang I – Grundlegende Cybersecurityanforderungen – konform sind.	✅	✅
Melden	Unverzügliche Information der Hersteller und der Marktüberwachungsbehörden, wenn das PDE ein erhebliches Cybersicherheitsrisiko darstellt.	✅	✅
	Information des Herstellers über jede Schwachstelle im Produkt	✅	✅
	Information der Marktüberwachungsbehörden und, soweit möglich, der Nutzenden, falls der Hersteller dieses Produkts seinen Betrieb eingestellt hat und daher nicht in der Lage ist, die Verpflichtungen gemäß des CRA zu erfüllen.	✅	✅
Selbstidentifizierung	Angabe der Kontaktdaten auf der PDE oder in den Begleitdokumenten des Produkts in einer Sprache, die für die Nutzenden und Marktüberwachungsbehörden leicht verständlich ist.	✅	
Aufbewahrung von Konformitätsdokumenten	Aufbewahrung einer Kopie der EU-Konformitätserklärung für mindestens 10 Jahre für die Marktüberwachungsbehörden.	✅	
Sicherstellen	Vor dem Inverkehrbringen eines Produkts:		
	(a) dass die entsprechenden Konformitätsbewertungsverfahren durchgeführt wurden;[9]	✅	
	(b) dass der Hersteller die technischen Unterlagen erstellt hat;	✅	
	(c) dass das Produkt für den Endverbraucher die CE-Kennzeichnung trägt und mit der EU-Konformitätserklärung sowie den in Anhang II aufgeführten Informationen und Anweisungen für den Benutzer in einer Sprache versehen ist, die für Benutzer und Marktüberwachungsbehörden leicht verständlich ist;[10]	✅	
	(d) dass das PDE oder seine Dokumentation eine Kennzeichnung des Produkts, des Herstellers und der Supportdauer enthält.[11]	✅	
	Der Hersteller und der Einführer erfüllen die Verpflichtungen und stellen dem Händler alle erforderlichen Unterlagen zur Verfügung.		✅

Tabelle 3: Pflichten von Einführern und Händlern

[9] *Wie in Artikel 32 festgelegt*
[10] *Gemäß Artikel 30 und Artikel 13 Absatz 20*
[11] *Gemäß Artikel 13 Absatz 15, 16 und 19*

Darüber hinaus sind in Artikel 21 die Umstände aufgeführt, unter denen die für Hersteller geltenden Verpflichtungen auch für Einführer und Händler gelten. Dies ist der Fall, wenn der Einführer oder Händler ein PDE unter seinem Namen oder seiner Marke in Verkehr bringt oder eine wesentliche Änderung an einem bereits in Verkehr gebrachten PDE vornimmt.

3.4 Andere natürliche oder juristische Personen (Artikel 22)

Artikel 22 befasst sich mit dem Fall, dass eine natürliche oder juristische Person (außer dem Hersteller, dem Einführer oder dem Händler) eine wesentliche Änderung an einem PDE vornimmt und dieses Produkt auf dem Markt bereitstellt. In diesem Fall gilt die betreffende Einrichtung als Hersteller.

3.5 Bevollmächtigte Vertreter in der EU

Eine weitere Rolle, in der KMU anerkannt werden können, ist die eines Bevollmächtigten des Herstellers. Diese Rolle leitet sich aus der Rolle des Herstellers ab und ist in einem besonderen Mandat definiert, mit dem der Hersteller den Bevollmächtigten bestellt. Das Mandat kann alle Aufgaben des Herstellers umfassen, mit Ausnahme derjenigen, die in Artikel 18 der CRA ausdrücklich genannt sind und sich hauptsächlich auf die Cybersicherheit während der Entwurfs-, Entwicklungs- und Produktionsphase beziehen. In Bezug auf die CRA-Anforderungen an die Cybersicherheit des Produkts, wenn es auf dem Markt ist, muss der Bevollmächtigte jedoch mit den Behörden zusammenarbeiten, die die von ihm vertretene PDE kontrollieren.

Hersteller können einen Bevollmächtigten benennen, der Aufgaben in ihrem Namen wahrnimmt – dies geschieht durch Erteilung eines Mandats an den Bevollmächtigten. Der Bevollmächtigte ist verpflichtet, den Marktüberwachungsbehörden auf Verlangen eine Kopie dieses Mandats vorzulegen.

Wenn sich der Hersteller dafür entscheidet, muss das Mandat dem Bevollmächtigten mindestens Folgendes ermöglichen:

- Die EU-Konformitätserklärung und die technischen Unterlagen (siehe Abschnitt 4 dieser Leitlinien) müssen den Marktüberwachungsbehörden mindestens 10 Jahre lang nach dem Inverkehrbringen des PDE oder während des Supportzeitraums, je nachdem, welcher Zeitraum länger ist, zur Verfügung stehen.
- Auf Verlangen sind den Marktüberwachungsbehörden alle Informationen und Unterlagen zur Verfügung zu stellen, die zum Nachweis der Konformität des PDE erforderlich sind;
- Zusammenarbeit mit den Marktüberwachungsbehörden.

3.6 Konformitätsbewertungsstellen

KMU könnten auch die Rolle von Konformitätsbewertungsstellen (CABs) übernehmen, die im CRA auch als notifizierte Stellen bezeichnet werden. Dabei handelt es sich um unabhängige Organisationen, die von den EU-Mitgliedstaaten benannt und der Europäischen Kommission

gemeldet werden, um Konformitätsbewertungen durch Dritte durchzuführen. Sie beurteilen, ob bestimmte digitale Produkte den Cybersicherheitsanforderungen entsprechen, bevor eine CE-Kennzeichnung beantragt werden kann.

CABs sind in erster Linie dafür verantwortlich, Konformitätsbewertungen gemäß den CRA-Anforderungen (Module B, C und H) durchzuführen und die entsprechenden technischen Unterlagen zu überprüfen. Bei einer erfolgreichen Bewertung stellt die benannte Stelle eine Konformitätserklärung aus, die für die CE-Kennzeichnung erforderlich ist.

Dementsprechend müssen Konformitätsbewertungsstellen:

- gemäß den EU-Vorschriften akkreditiert und benannt sein.[12]
- technisch kompetent in den Bereichen Cybersicherheit und Produktbewertung sein.

Sie unterliegen der nationalen Aufsicht und der Koordinierung auf EU-Ebene.

[12] NANDO (New Approach Notified and Designated Organisations) Informationssystem https://webgate.ec.europa.eu/single-market-compliance-space/notified-bodies

4. Grundlegende Anforderungen an die Cybersicherheit

4.1 In Bezug auf die Eigenschaften von Produkten

4.1.1 Grundsätze „Sicherheit durch Design“ und „Sicherheit durch Standardeinstellungen“

Die CRA-Anforderungen zur Übernahme des Grundsatzes „Secure by Design“ und „Secure by Default“ werden an mehreren Stellen im Text erwähnt:

- In Erwägungsgrund 32 der CRA wird anerkannt, dass *„Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sowie die Cybersicherheit im Allgemeinen sind Schlüsselelemente der Verordnung (EU) 2016/679“* sind.[13]
- In Erwägungsgrund 34 heißt es*: „Wenn die Hersteller in der Entwurfs- und Entwicklungsphase von Dritten bezogene Komponenten in Produkte mit digitalen Elementen integrieren, sollten sie in Bezug auf diese Komponenten, einschließlich freier und quelloffener Softwarekomponenten, die nicht auf dem Markt bereitgestellt wurden, die gebotene Sorgfalt walten lassen, um sicherzustellen, dass die Produkte im Einklang mit den in dieser Verordnung festgelegten grundlegenden Cybersicherheitsanforderungen konzipiert, entwickelt und hergestellt werden.“*
- Artikel 13 Absatz 1, in dem die Pflichten der Hersteller aufgeführt sind, verlangt: *„Wenn sie ein Produkt mit digitalen Elementen in den Verkehr bringen, gewährleisten die Hersteller, dass dieses Produkt gemäß den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I konzipiert, entwickelt und hergestellt worden ist.“*
- Anhang I, in dem die grundlegenden Cybersicherheitsanforderungen aufgeführt sind, verlangt*: „(1) Produkte mit digitalen Elementen werden so konzipiert, entwickelt und hergestellt, dass sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten.“*

13Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR)

Als Nachweis für die Einhaltung des Grundsatzes „Sicherheit durch Design“ können KMU den Risikomanagementplan für die Produktentwicklung verwenden, der Strategien zur Risikoerkennung, -analyse und -minderung für jede Entwicklungsphase umfasst.

Ausdrücklicher formuliert enthält Anhang I Nummer 2 Buchstabe b eine ausdrückliche Anforderung an eine sichere Standardkonfiguration: *„Produkte mit digitalen Elementen müssen: b) mit einer sicheren Standardkonfiguration auf dem Markt bereitgestellt werden, sofern zwischen dem Hersteller und dem gewerblichen Nutzer in Bezug auf ein maßgeschneidertes Produkt mit digitalen Elementen nichts anderes vereinbart wurde, und die Möglichkeit bieten, das Produkt in seinen ursprünglichen Zustand zurückzusetzen.“*

Diese Begriffe werden im Text nicht definiert, und ihre Bedeutung wird als selbstverständlich vorausgesetzt. Die deutsche Regulierungsbehörde – das Bundesamt für Sicherheit in der Informationstechnik (BSI)[14] – erläutert beispielsweise, dass das CRA-Prinzip „Security by Design“ bedeutet, dass *„vernetzte Produkte im Hinblick auf Cybersicherheit konzipiert werden, z.B. indem sichergestellt wird, dass die mit dem Produkt gespeicherten oder übertragenen Daten verschlüsselt sind und die Angriffsfläche so gering wie möglich ist.“*, und dass das Prinzip „Security by Default“ bedeutet, dass *„die Standardeinstellungen vernetzter Produkte zur Erhöhung deren Sicherheit beitragen, z.B. durch das Verbot schwacher Standardpasswörter, durch die automatische Installation von Sicherheitsupdates usw.“.*

Was akzeptable Nachweise für die Einhaltung des „Secure-by-Default“-Prinzips angeht, sollten KMU erwägen, die durchgesetzten Regeln für die sichere Konfiguration zu dokumentieren und, wenn es sich um ein maßgeschneidertes Produkt handelt, eine angemessene Vereinbarung mit seinen Geschäftskunden mit entsprechenden Klauseln anzubieten.

In der Praxis muss die Auslegung dieser Anforderungen auf der Risikobewertung basieren und liegt im Ermessen des Herstellers, wobei die Art des Produkts und der Kontext, in dem es eingesetzt wird, zu berücksichtigen sind.

4.1.2 Cybersicherheits-Risikomanagement

Die Bewertung von Cybersicherheitsrisiken bildet die Grundlage für den gesamten Ansatz zur Cybersicherheit, der in der CRA dargelegt ist, und fördert einen proaktiven Ansatz für das Risikomanagement, der die Cybersicherheitsmaßnahmen rechtfertigt, im Gegensatz zu einem Compliance-Ansatz.[15] Die Risikobewertung ist ein Eckpfeiler der Produktsicherheit und bietet eine systematische Methode zur Identifizierung, Bewertung und Priorisierung potenzieller Bedrohungen von den frühesten Entwicklungsstadien bis zum gesamten Produktlebenszyklus. Durch die kontinuierliche Aktualisierung der Risikobewertung im Zuge der Produktentwicklung stellen Unternehmen sicher, dass die Sicherheitsmaßnahmen robust und relevant bleiben und sowohl das Produkt als auch seine Nutzer wirksam schützen. Dieser Prozess dient nicht nur als

[14] BSI – Bundesamt für Sicherheit in der Informationstechnik in Deutschland (2025) Cyber-Resilienz-Gesetz, abrufbar unter: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html#:~:text=Take%20cybersecurity%20into%20account,not%20have%20to%20be%20published.. abgerufen am 21. Juli 2025

[15] Auf das Risikomanagement wird auch in den Erwägungsgründen 37, 38, 39, 48 und 52 (in Bezug auf die auf Unionsebene koordinierte Bewertung der Sicherheitsrisiken kritischer Lieferketten), 53, 55, 58 und 114 Bezug genommen.

Leitfaden für die Auswahl und Strenge von Sicherheitskontrollen, sondern bildet auch die Grundlage für alle nachfolgenden Sicherheitsbewertungen und -entscheidungen. Die Einhaltung bewährter Verfahren – wie sie beispielsweise in ISO 31000 oder ISO 14971 beschrieben sind – gewährleistet einen umfassenden und wiederholbaren Ansatz. Letztendlich ist die Risikobewertung nicht nur für die Entwicklung sicherer Produkte unerlässlich, sondern auch eine zwingende Voraussetzung für die Einhaltung der CRA und aller anderen EU-Vorschriften zur Cybersicherheit oder Sicherheit. Tatsächlich verwendet die CRA selbst Risikobewertungstechniken, um eine Reihe von Produktklassen zu definieren und Sicherheitsanforderungen festzulegen, die das mit jeder Produktklasse verbundene Risikoniveau widerspiegeln. Eine Vorlage für die Risikobewertung finden Sie in Anhang B dieses Dokuments.

Darüber hinaus handelt es sich bei der Risikobewertung für PDE gemäß CRA um eine produktspezifische Bewertung, die über einzelne Projekt- oder Organisationsrisikobewertungen hinausgeht. Um die CRA-Anforderungen zu erfüllen, muss die Bewertung speziell auf die Sicherheit folgender Aspekte eingehen:

- **Sicherheit der Endnutzer**, d. h. Informationen und Anweisungen, die dem Nutzer zur Verfügung gestellt werden müssen,
- **Bewertung der Risiken in der Lieferkette**, einschließlich der durch die Software-Stückliste (SBOM) identifizierten Schwachstellen, unter anderem durch die Erstellung einer Software-Stückliste in einem gängigen und maschinenlesbaren Format, die mindestens die obersten Abhängigkeiten der Produkte abdeckt, und durch Berücksichtigung der SBOM in den unten diskutierten Anforderungen an das Schwachstellenmanagement, und
- **Berücksichtigung der Auswirkungen,** die die PDE oder die mit ihr verbundenen Geräte auf andere Netzwerke und Produkte haben könnten, mit denen sie interagieren, d. h. die unten erörterten Produktdesignanforderungen.

Diese umfassende Perspektive stellt sicher, dass nicht nur das Produkt selbst, sondern auch sein Ökosystem und seine Nutzer vor sich entwickelnden Bedrohungen geschützt sind und dass die Sicherheitskontrollen auf die realen, miteinander verbundenen Risiken zugeschnitten sind.

Die wichtigsten Verweise im CRA-Text sind:

- ➔ Artikel 3(37) und 3(38) definieren die Begriffe „Cybersicherheitsrisiko“ und „erhebliches Cybersicherheitsrisiko“.
- ➔ Artikel 13 enthält ausdrückliche Anforderungen, wie Hersteller das Risikomanagement durchführen sollten, um ein angemessenes Sicherheitsniveau für ihre Produkte zu gewährleisten. In Absatz 13(3) sind die Komponenten aufgeführt, die mindestens enthalten sein müssen, wie z. B. die Risikoanalyse auf der Grundlage des beabsichtigten Verwendungszwecks und der vorhersehbaren Verwendung, die Verwendungsbedingungen wie die Betriebsumgebung oder die zu schützenden Vermögenswerte und andere.
- ➔ Anhang I (Punkt 2) legt eine Reihe wesentlicher Cybersicherheitsanforderungen auf der Grundlage der in Artikel 13 Absatz 2 genannten Cybersicherheitsrisikobewertung fest.

4.1.3 Sicherheitsziele

Die Produktsicherheit ist ein Eckpfeiler des Cyber Resilience Act, der von Unternehmen verlangt, robuste Sicherheitsmaßnahmen während des gesamten Produktlebenszyklus zu implementieren, vom Design und der Entwicklung bis hin zur Bereitstellung und Wartung. Zu den wichtigsten Bereichen gehören:

- **Identitäts- und Zugriffsmanagement**: Sicherstellen, dass nur autorisierte Benutzer und Systeme auf sensible Funktionen und Daten zugreifen können, um das Risiko von unbefugtem Zugriff und Missbrauch zu verringern.
- **Protokollierung**: Implementierung einer umfassenden Protokollierung zur Überwachung von Aktivitäten, Erkennung von Anomalien und Unterstützung forensischer Untersuchungen im Falle von Vorfällen;
- **Datensicherheit und -minimierung**: Schutz der Daten in jeder Phase und Erfassung nur der unbedingt notwendigen Daten, wodurch die Gefährdung begrenzt und Compliance-Risiken reduziert werden.
- **Sicherung und sichere Löschung**: Regelmäßige Sicherung kritischer Daten und Sicherstellung der sicheren Löschung, wenn Daten nicht mehr benötigt werden, um Datenverlust und unbefugte Wiederherstellung zu verhindern.
- **Verschlüsselung**: Schutz von Informationen während der Übertragung und im Ruhezustand, wodurch Daten für Unbefugte unlesbar werden und somit die Vertraulichkeit gewahrt bleibt.

Durch die Integration dieser Kontrollen über den gesamten Produktlebenszyklus hinweg können Unternehmen die CRA-Anforderungen erfüllen, das Vertrauen stärken und die Nutzer vor sich entwickelnden und neu auftretenden Cyber-Bedrohungen schützen.

In Anhang I des CRA sind unter Punkt (2) spezifische Sicherheitsziele aufgeführt, die vom Hersteller umgesetzt werden müssen, wobei jedoch die Einzelheiten der Umsetzung dieser Mechanismen die für das Produkt durchgeführte Risikobewertung widerspiegeln müssen. Diese Kontrollmechanismen umfassen Praktiken, Verfahren und technische Maßnahmen – die wichtigsten von ihnen werden im Folgenden kurz erläutert.

Anforderungen an das Produktdesign

Die Produkte müssen:

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

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

Diese Anforderungen an die Konstruktion sollten zusammen mit der Anforderung einer standardmäßig sicheren Konfiguration betrachtet werden.

Als Nachweis für die Einhaltung der oben genannten Anforderungen sollten KMU umfassende Produktrisikobewertungen einführen, umsetzen und überwachen, Risiken auf Dienste und Kontrollen abbilden, die Konstruktionsdokumentation bewerten, Codeüberprüfungen durchführen, getrennte Produktions- und Entwicklungsumgebungen sicherstellen, Sicherheitsbaselines festlegen und überwachen, um Anomalien zu finden, und regelmäßige Backups von Software und Daten durchsetzen.

Maßnahmen zur Erkennung und Beseitigung von Schwachstellen während des gesamten Produktlebenszyklus

Die Erkennung und Beseitigung von Schwachstellen vor der Veröffentlichung der Software ist eine zentrale Anforderung der CRA

Produkte mit digitalen Elementen müssen:

„(a) ohne bekannte ausnutzbare Schwachstellen auf dem Markt bereitgestellt werden“.

Bekannte Schwachstellen sind in öffentlichen Schwachstellendatenbanken aufgeführt, beispielsweise in der EU-Schwachstellendatenbank,[16] der US-amerikanischen National Vulnerability Database[17] oder den Schwachstellenscan-Tools (weitere Einzelheiten zum Schwachstellenscan und -management finden Sie in der Confirmate-Pentesting-Methodik).

Wenn bekannt wird, dass eine Schwachstelle bereits für einen Cyberangriff ausgenutzt wurde, muss der Hersteller die erforderlichen Maßnahmen ergreifen, um zu verhindern, dass sie vor und nach dem Inverkehrbringen erfolgreich gegen das PDE ausgenutzt wird. Viele Hacker, auch solche ohne fortgeschrittene Kenntnisse, nutzen noch nicht gepatchte, aber bekannte Schwachstellen durch Zero-Day-Exploits aus. Daher müssen PDE

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

Der zweite Teil der grundlegenden Sicherheitsanforderungen ist vollständig dem Umgang mit Schwachstellen gewidmet.

Sobald eine Schwachstelle identifiziert wurde, ist es wichtig, sie gemäß einem anerkannten Rahmenwerk wie CVSS (Common Vulnerability Scoring System) nach ihrem Schweregrad zu bewerten. Die Priorisierung erfolgt anhand dieser Bewertung, sodass kritische und aktiv ausgenutzte Schwachstellen mit Dringlichkeit behoben werden. Die Behebung erfolgt in der Regel durch die Veröffentlichung eines Patches oder einer Konfigurationsänderung.

Gemäß CRA sind Hersteller eindeutig verpflichtet, diese Sicherheitsupdates ohne unnötige Verzögerung unter Verwendung sicherer Update-Mechanismen an die Benutzer zu übermitteln und dies getrennt von Funktionsupdates zu tun. Updates müssen kostenlos bereitgestellt

[16] Verfügbar unter: https://euvd.enisa.europa.eu/
[17] Verfügbar unter: https://nvd.nist.gov/

werden, mit klaren Hinweisen versehen sein und, soweit möglich, standardmäßig für die automatische Installation aktiviert sein. Dadurch wird sichergestellt, dass Benutzer umgehend geschützt sind, auch wenn sie nicht proaktiv handeln. Als Best Practice in der Branche werden Service Level Agreements (SLAs) für das Patch-Management empfohlen. Zum Beispiel:

- 24 bis 48 Stunden für das Patchen kritischer Schwachstellen
- 7 Tage für hohe Schwachstellen
- 30 Tage für mittlere Schwachstellen
- 90 Tage für geringe Schwachstellen

Nach der Behebung ist eine kontinuierliche Überwachung unerlässlich. Hersteller sollten sicherstellen, dass Patches effektiv angewendet wurden, und auf Versuche achten, verbleibende Schwachstellen auszunutzen. Dazu gehört die Analyse von Systemprotokollen und die Beachtung von Warnmeldungen zur Intrusion Detection.

Zu vermeidende Fallstricke:

- Aufschieben der Behebung bis zur Aktualisierung der Funktionen
- Unterschätzung der Schwere der Schwachstellen
- Versäumnis, die Benutzer rechtzeitig und in verständlicher Weise zu informieren

Darüber hinaus kann die überstürzte Installation von Patches ohne ordnungsgemäße Tests neue Probleme oder Risiken mit sich bringen. Durch die Kombination von sofortigen Abhilfemaßnahmen, Patch-Bereitstellung und kontinuierlicher Überwachung können KMU einen robusten Schwachstellenmanagementprozess etablieren, der die wesentlichen Cybersicherheitsanforderungen der CRA erfüllt.

Empfohlene Nachweise für die Einhaltung der oben genannten Anforderungen könnten neben der Entwicklung und Durchsetzung relevanter Richtlinien und Verfahren auch Penetrationstests (intern und durch Dritte), automatische Sicherheitsupdate-Mechanismen, Code-Überprüfungen und vor allem relevante (sogar proaktive) Updates in angemessener Zeit umfassen, sobald eine neue Bedrohung oder Schwachstelle bekannt wird, auch wenn diese noch nicht ausgenutzt wurde.

<u>Technische Anforderungen</u>
Beispiele für typische Maßnahmen zur Erfüllung der technischen Anforderungen des CRA sind in allen Informationssicherheitsstandards aufgeführt, darunter NIST SP800 oder Cyber Fundamentals (CyFun), jeweils unter dem Thema Protect. Beispiele für spezifische Maßnahmen sind nachstehend aufgeführt.

Der CRA sieht vor, dass PDE
„(d) durch geeignete Kontrollmechanismen Schutz vor unbefugtem Zugriff bieten, darunter u. a. zumindest Authentifizierungs-, Identitäts- oder Zugangsverwaltungssysteme, und einen möglicherweise unbefugten Zugriff melden“.
Zu den relevanten empfohlenen Maßnahmen des NIST Cybersecurity Framework gehören:

- Erfordernis einer Multi-Faktor-Authentifizierung;
- Durchsetzung von Richtlinien für die Mindeststärke von Passwörtern, PINs und ähnlichen Authentifizierungsmitteln;
- Regelmäßige erneute Authentifizierung von Benutzern, Diensten und Hardware auf der Grundlage des Risikos (z. B. in Zero-Trust-Architekturen);
- Sicherstellen, dass autorisiertes Personal unter Notfallbedingungen auf Konten zugreifen kann, die für den Schutz der Sicherheit unerlässlich sind.

Laut CRA müssen PDE außerdem
„(e) die Vertraulichkeit gespeicherter, übermittelter oder anderweitig verarbeiteter personenbezogener oder sonstiger Daten schützen, z. B. durch Verschlüsselung relevanter Daten, die gespeichert sind oder gerade verwendet oder übermittelt werden, durch modernste Mechanismen und durch den Einsatz anderer technischer Mittel.“
Relevante Leitlinien zu Cyber-Grundlagen als Maßnahmen umfassen:

- Erwägung des Einsatzes von Verschlüsselungstechniken für die Datenspeicherung, Datenübertragung oder den Datentransport (z. B. Laptop, USB);
- Modernste Mechanismen zur Integritätsprüfung (z. B. Paritätsprüfungen, zyklische Redundanzprüfungen, kryptografische Hash-Funktionen) und zugehörige Tools können die Integrität von Informationssystemen und gehosteten Anwendungen automatisch überwachen.

Ähnliche Leitlinien finden sich auch in anderen relevanten Normen im CRA, denen zufolge PDE:

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

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

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

Es ist wichtig zu beachten, dass der CRA festlegt, *was* zu tun ist, aber nicht, *wie* es zu tun ist. Die Art und Weise, wie die Anforderungen umgesetzt werden, liegt vollständig im Ermessen des Herstellers, obwohl eindeutig erwartet wird, dass die angewandten Methoden dem mit dem Produkt verbundenen Risikoniveau angemessen sind.

KMU könnten die Einhaltung der oben genannten Anforderungen nachweisen, indem sie ihre Produkte mit digitalen Elementen mit Protokollierungsfunktionen ausstatten, die eine Integration in die Cybersicherheitsumgebung ihrer Geschäftsanwender ermöglichen. Bei der Integration

sollte auch die Kompatibilität mit einer zentralisierten Zugriffskontrolle berücksichtigt werden, die regelmäßig getestet wird, einschließlich Penetrationstests, und nicht zuletzt – fortschrittliche Kryptografie.

Zu den spezifischen Sicherheitsmaßnahmen, die KMU mindestens berücksichtigen sollten, um die oben genannten Anforderungen zu erfüllen, gehören:

- Einführung von Richtlinien und Verfahren für Identitäts-, Zugriffskontrolle, Autorisierung und Vorfallmanagement.
- Implementierung spezieller Sicherheitsvorkehrungen, um unbefugten Zugriff, Verfälschung oder Änderung von Systemdaten und Audit-Aufzeichnungen zu verhindern (z. B. eingeschränkte Zugriffsrechte, tägliche Backups, Datenverschlüsselung, Installation von Firewalls).
- Implementierung von Mechanismen zur Integritätserkennung und Berichterstattung.
- Aktivierung der Multi-Faktor-Authentifizierung.
- Durchsetzung von Richtlinien für die Mindeststärke von Passwörtern, PINs und ähnlichen Authentifizierungsmitteln.
- Implementierung von Mechanismen zur Erkennung und Reaktion auf DDoS-Angriffe.

<u>Maßnahmen zur Minimierung der Auswirkungen auf die IT-Umgebung</u>

Es gibt zwei CRA-Anforderungen, die darauf abzielen, die Auswirkungen eines Vorfalls oder einer Fehlfunktion des Produkts auf seine Umgebung zu minimieren, nämlich die unten beschriebenen Punkte (i) und (k):

Laut (i) müssen die PDE

„die negativen Auswirkungen von den Produkten selbst oder von vernetzten Geräten auf die Verfügbarkeit der von anderen Geräten oder Netzen bereitgestellten Dienste minimieren“.

Diese Anforderung schreibt vor, dass PDEs nicht nur für ihr eigenes Konto sicher sind, sondern auch keine Gefahr für die Verfügbarkeit anderer Geräte oder Netzwerke darstellen. Dies ähnelt der Funkgeräterichtlinie, wonach Geräte andere Geräte oder Netzwerke nicht stören dürfen, sodass Geräte das Funkfrequenzspektrum effizient nutzen und elektromagnetische Verträglichkeitsstandards erfüllen müssen, um schädliche Störungen zu vermeiden. In Bezug auf die Cybersicherheit empfehlen wir, dass PDEs sorgfältig konzipiert werden, um beispielsweise einen übermäßigen Daten-, CPU- oder Netzwerkverbrauch zu vermeiden, und dass sie über Kontrollpunkte verfügen, um zu verhindern, dass sie für Denial-of-Service-Angriffe genutzt werden. Bei einem Denial-of-Service-Angriff könnten kompromittierte PDEs in eine Armee von Bots (kompromittierte Geräte) aufgenommen werden, die gleichzeitig ein Netzwerk, eine Website oder eine Anwendung angreifen und das angegriffene Produkt oder Netzwerk lahmlegen.

Laut (k) müssen PDE

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

Zu den spezifischen Sicherheitsmaßnahmen, die KMU mindestens berücksichtigen sollten, um die oben genannten Anforderungen zu erfüllen, gehören:

- Durchführung einer umfassenden Produktrisikobewertung seit der Entstehungsphase, einschließlich Überlegungen zu den potenziellen Risiken für die Verfügbarkeit von Diensten, die von anderen Geräten oder Netzwerken bereitgestellt werden, aufgrund des PDE oder der verbundenen Geräte, und Ermittlung von Maßnahmen zur Minderung der Auswirkungen oder Wahrscheinlichkeit des Risikos.
- Implementierung spezieller Sicherheitsvorkehrungen, um unbefugten Zugriff, Verfälschung oder Änderung von Systemdaten und Audit-Aufzeichnungen zu verhindern (z. B. eingeschränkte Zugriffsrechte, tägliche Backups, Datenverschlüsselung, Installation von Firewalls).
- Implementierung von Mechanismen zur Erkennung und Reaktion auf DDoS-Angriffe.

Benutzerbezogene Kontrollen

Zwei zusätzliche Maßnahmen zielen darauf ab, den Benutzer in die Lage zu versetzen, seine eigene Sicherheit und seine Daten zu verwalten. Laut CRA sollen PDE

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

Die Techniken zur Erkennung von abnormalem Verhalten, das auf einen Cyberangriff hindeutet, basieren meist auf der Überprüfung und Analyse von Protokollen der Produkte mit digitalen Elementen, um die Art und den Vektor des Angriffs zu bestimmen und geeignete Maßnahmen zur Reaktion zu ergreifen. Dies geschieht in der Regel mit automatisierten Tools zum Sammeln und Korrelieren von Protokollen, für die die Produkte mit digitalen Elementen über die unterstützende Funktionalität zur Aufzeichnung und Überwachung ihrer Aktivitäten verfügen müssen.

Weiterhin sollen PDE

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

Es gibt verschiedene Techniken zur sicheren Datenlöschung, je nach Art des Datenträgers (Papier, Laufwerk, Cloud) oder Sensibilitätsstufe (von allgemeinen Daten bis hin zur Kundenhistorie).

Zu den spezifischen Sicherheitsmaßnahmen, die KMU mindestens berücksichtigen sollten, um die oben genannten Anforderungen zu erfüllen, gehören:

- Integration von Unterstützungsfunktionen für die Aufzeichnung und Überwachung von PDE-Aktivitäten.
- Integration von Funktionen zum sicheren Löschen und Übertragen von Daten sowie einer Möglichkeit für den Benutzer, den Vorgang auf einfache Weise zu starten.

- Verwendung von Methoden wie vollständiges Überschreiben des Speichers, verschlüsselungsbasiertes Löschen, Zero-Fill, Löschen auf Hardware-Ebene oder sogar physische Zerstörung, um sicherzustellen, dass die Daten wirklich nicht wiederherstellbar sind. Es ist von entscheidender Bedeutung, vor dem Löschen alle gespeicherten sensiblen Daten zu identifizieren, zu überprüfen, ob sie tatsächlich gelöscht wurden, und während des Prozesses die Gerätezertifikate zu widerrufen.

CRA geht davon aus, dass Hacker wichtige (oder sogar vertrauliche) Informationen für die Planung ihrer Angriffe erhalten können, die sie aus PDEs extrahieren können, auf die sie Zugriff erhalten, nachdem diese ausgemustert oder durch andere ersetzt wurden, es sei denn, es gibt einen sicheren Mechanismus zur sicheren Vernichtung der alten Daten und zur Bereinigung der ausrangierten Datenspeicher.

4.2 Sicherheit in Lieferketten und bei Dritten

Die Hersteller sind für die Cybersicherheit des gesamten von ihnen hergestellten Produkts verantwortlich, einschließlich aller eingebetteten oder integrierten Komponenten von Drittanbietern, wie Softwarebibliotheken, Open-Source-Module und Firmware. Insbesondere müssen Hersteller die von der Lieferkette ausgehenden Risiken bewerten und verwalten und überprüfen, ob die Software von Drittanbietern den CRA-Anforderungen entspricht.

In der Praxis bedeutet dies, dass jede dem Hersteller auferlegte Verantwortung auch von der entsprechenden Lieferkette erwartet werden muss, wenn sie Auswirkungen auf das Endprodukt hat. Beispiele für Erwartungen sind unter anderem:

- Sicherheit durch Design und Standard;
- Verlängerung der Supportdauer (muss mit der des Endprodukts kompatibel sein);
- Umgang mit Schwachstellen und Offenlegung;
- Umgang mit Vorfällen (soweit diese Auswirkungen auf das Produkt des Herstellers haben).

Infolgedessen wird von den Herstellern erwartet, dass sie bei der Auswahl von Lieferanten und anderen Drittanbietern, die zu ihren Produkten beitragen, die erforderliche Sorgfalt walten lassen.

Im diesem Zusammenhang müssen Hersteller eine Software-Stückliste (Software Bill of Materials, SBOM) führen und bereitstellen, in der alle verwendeten Softwarekomponenten, einschließlich Abhängigkeiten von Drittanbietern und Open-Source-Komponenten, aufgeführt sind. Die SBOM muss

- auf Anfrage von Kunden und Marktüberwachungsbehörden in maschinenlesbarer Form verfügbar sein;
- auf dem neuesten Stand gehalten werden und alle Änderungen während des gesamten Produktlebenszyklus widerspiegeln.

Weitere Einzelheiten zum Format (z. B. JSON) und zu den Elementen (Informationen) der SBOM können von der Europäischen Kommission in Form eines Durchführungsrechtsakts bereitgestellt werden.

Parallel dazu gibt die US-Behörde für Cybersicherheit und Infrastruktursicherheit (CISA) in ihrem Entwurf „Minimum Elements for a Software Bill of Materials (SBOM)" von August 2025 einen Einblick in bewährte Verfahren und Mindestanforderungen.

Für KMU, die Produkte herstellen, die unter den CRA fallen, geben diese sich weiterentwickelnden SBOM-Anforderungen der CISA Aufschluss über die technischen Aspekte und Standards für die Pflege der SBOM. Die Details der CISA führen jedoch auch zu einer nicht unerheblichen operativen Komplexität.

4.3 Schwachstellenmanagement

Teil II der grundlegenden Sicherheitsanforderungen (Anhang I der CRA) befasst sich mit den Anforderungen an die Behandlung von Schwachstellen. Hier gibt es einige Überschneidungen mit den Anforderungen von Teil I (z. B. die Anforderung, dass Produkte mit digitalen Elementen ohne bekannte ausnutzbare Schwachstellen auf den Markt gebracht werden müssen). Die meisten der in diesem Teil des Anhangs aufgeführten Anforderungen sind jedoch richtlinien- und verfahrensorientiert und zielen ausdrücklich auf das Schwachstellenmanagement ab.

4.3.1 Identifizierung und Dokumentation

Laut Teil II des Anhang 1 des CRA müssen Hersteller
(1) Schwachstellen und Komponenten der Produkte mit digitalen Elementen ermitteln und dokumentieren, u. a. durch Erstellung einer Software-Stückliste in einem gängigen maschinenlesbaren Format, aus der zumindest die obersten Abhängigkeiten der Produkte hervorgehen".
Die Erstellung einer Software-Stückliste (SBOM) ist obligatorisch. Weitere Informationen darüber, wie das Konzept der SBOM mit der CRA zusammenhängt, finden sich in den Erwägungsgründen 77 und 118 sowie in Artikel 13 Absatz 24 des CRA.
Wie oben erwähnt, gibt es zum Zeitpunkt der Abfassung dieses Dokuments weder ein vorgeschriebenes Format für ein solches Dokument noch ein anerkanntes Standardformat, obwohl Artikel 13 Absatz 24 der Kommission ermöglicht, durch Durchführungsrechtsakte unter Berücksichtigung europäischer oder internationaler Normen und bewährter Verfahren das Format und die Elemente der SBOM festzulegen.
Darüber hinaus müssen Hersteller laut Teil II *„(3) die Sicherheit des Produkts mit digitalen Elementen regelmäßig und wirksam testen und überprüfen".*
Hier ist es wichtig zu beachten, dass die Anforderung (3) darin besteht, einen umfassenden und regelmäßigen Prozess zur Prüfung und Überprüfung sowohl technischer als auch organisatorischer Schwachstellen und Fehlkonfigurationen einzurichten, unabhängig davon, ob eine Schwachstelle entdeckt wurde oder nicht.

4.3.2 Behebung

Die PDE-Schwachstellen müssen unverzüglich behoben oder beseitigt werden. Dies ist erforderlich, um sicherzustellen, dass das Produkt auf dem EU-Markt sicher bleibt. Darüber hinaus hat der CRA festgelegt, dass neue Sicherheitsupdates, soweit möglich, getrennt von

Funktionsupdates bereitgestellt werden müssen. Dies könnte dazu beitragen, den zeitlichen Unterschied zwischen Produktentwicklung und Sicherheitswartung zu verringern.

4.3.3 Offenlegung von Schwachstellen und Informationsaustausch

In diesem Bereich gibt es drei wesentliche Anforderungen, die im Teil II des Anhang 1 beschrieben werden. Entsprechend dieser müssen Hersteller von PDE:
„(4) sobald eine Sicherheitsaktualisierung bereitgestellt worden ist, Informationen über beseitigte Schwachstellen teilen und veröffentlichen, einschließlich einer Beschreibung der Schwachstellen mit Angaben, anhand deren die Nutzer das betroffene Produkt mit digitalen Elementen, die Auswirkungen der Schwachstellen und ihre Schwere erkennen können, sowie eindeutige und verständliche Informationen, die den Nutzern helfen, die Schwachstellen zu beheben; in hinreichend begründeten Fällen, in denen die Hersteller der Auffassung sind, dass die Risiken der Veröffentlichung die Vorteile in Bezug auf die Sicherheit überwiegen, können sie die Veröffentlichung von Informationen über eine behobene Schwachstelle so lange aufschieben, bis den Nutzern die Möglichkeit gegeben wurde, den entsprechenden Patch anzuwenden.
(5) eine Strategie für die koordinierte Offenlegung von Schwachstellen aufstellen und umsetzen;
(6) Maßnahmen ergreifen, um den Austausch von Informationen über mögliche Schwachstellen in ihrem Produkt mit digitalen Elementen und darin enthaltenen Komponenten Dritter zu erleichtern, und dazu u. a. eine Kontaktadresse für die Meldung der in dem Produkt mit digitalen Elementen entdeckten Schwachstellen angeben“.

Anforderung (5) bezieht sich auf die koordinierte Offenlegung von Sicherheitslücken, die in diesem Zusammenhang eine bestimmte Bedeutung hat. Das Konzept der koordinierten Offenlegung von Sicherheitslücken (CVD) wird von der ENISA ausführlich beschrieben.[18] Im Wesentlichen handelt es sich bei CVD um eine Reihe von Regeln (z. B. Richtlinien), die von einem Hersteller veröffentlicht werden und es externen Sicherheitsexperten mit guten Absichten (z. B. „ethischen Hackern“ oder Anbietern von Schwachstellenscans) ermöglichen, potenzielle Sicherheitslücken in seinen Systemen oder Produkten zu identifizieren, und die ein Verfahren (Formular, Kanal, Kontakte) zur Meldung der identifizierten Sicherheitslücken an den Hersteller vorsehen. Eine CVD legt in der Regel fest, welche Systeme in den Anwendungsbereich fallen und unter welchen Bedingungen die Identifizierung erfolgen kann (keine Gesetzesverstöße, keine Schäden, keine Datenlecks).

4.3.4 Verwaltung von Sicherheitsupdates

Die letzten Anforderungen von Teil II befassen sich mit der Verwaltung von Sicherheitsupdates und stellen sicher, dass die oben beschriebenen Abhilfemaßnahmen (Sicherheitsupdates) durch *„Mechanismen für die sichere Verbreitung von Aktualisierungen“* (7) für PDEs durchführbar sind. Punkt (8) sieht außerdem vor, dass Hersteller
„dafür sorgen, dass Sicherheitsaktualisierungen, die zur Bewältigung festgestellter Sicherheitsprobleme zur Verfügung stehen, unverzüglich und — sofern zwischen dem Hersteller und dem gewerblichen Nutzer in Bezug auf ein maßgeschneidertes Produkt mit digitalen

[18] https://www.enisa.europa.eu/topics/vulnerability-disclosure

Elementen nichts anderes vereinbart wurde — kostenlos verbreitet werden, zusammen mit Hinweisen und einschlägigen Informationen, auch über zu treffende mögliche Maßnahmen.“
All dies hat das Ziel, den Benutzern von PDEs zu ermöglichen, ihre Produkte sicher zu halten und bei Bedarf die erforderlichen Maßnahmen zur Risikominderung zu ergreifen.

5. Konformitätsbewertung

5.1 Konformitätsbewertungsverfahren

Die von der CRA angewandten Konformitätsbewertungsverfahren basieren auf dem New Legislative Framework (NLF)[19] und orientieren sich am Prinzip „hohes Risiko = hohe Sicherheit“. Das bedeutet, dass Standardkategorien (die in der Verordnung nicht ausdrücklich genannt sind) Selbstbewertungsverfahren unterliegen, die Kategorie „Wichtig I“ auf harmonisierten Normen oder einer Bewertung durch Dritte basiert und die Kategorien „Wichtig II“ und „Kritisch“ einer Bewertung und Zertifizierung durch Dritte unterliegen. Die spezifischen Anforderungen für die einzelnen Produktklassen sind in der folgenden Tabelle zusammengefasst. Eine detaillierte Beschreibung der Konformitätsbewertungsverfahren findet sich im Kapitel „CRA-Konformitätsprozess“ des Dokuments **CONFIRMATE D3.1 – Architecture for Automated CRA Conformance Assessment,** im CRA-Konformitätsprozess. Die Anforderungen sind in Artikel 32 des Gesetzes festgelegt. Anhang VIII enthält eine detaillierte Beschreibung der Konformitätsbewertungsverfahren selbst.

Die CRA erkennt die unten aufgeführten Konformitätsverfahren an und stützt sich auf diese.

5.1.1 Harmonisierte Normen. Hierbei handelt es sich um offiziell anerkannte europäische Normen, die die Konformität mit bestimmten rechtlichen Anforderungen der EU-Gesetzgebung vermuten lassen. Sie dienen als verbindliche, überprüfbare Grundlagen für das Risikomanagement, die sichere Entwicklung und die Betriebssicherheit.

Diese Normen müssen noch entwickelt und offiziell anerkannt werden, um die Konformität mit den grundlegenden Cybersicherheitsanforderungen zu vermuten. Im Februar 2025 beauftragte die EU-Kommission die europäischen Normungsgremien (CEN, CENELEC, ETSI) mit der

[19] Der NLF (New Legislative Framework) präzisiert die Verwendung der CE-Kennzeichnung und schafft einen Maßnahmenkatalog für die Produktgesetzgebung. Der NLF besteht aus: der Verordnung (EG) Nr. 765/2008 zur Festlegung der Anforderungen für die Akkreditierung und Marktüberwachung von Produkten und dem Beschluss Nr. 768/2008 über einen gemeinsamen Rahmen für die Vermarktung von Produkten, der Verweisbestimmungen enthält, die in die Überarbeitung der Produktgesetzgebung aufgenommen werden sollen. Im Grunde handelt es sich um eine Vorlage für künftige Rechtsvorschriften zur Harmonisierung von Produkten, die Verordnung (EU) 2019/1020 über die Marktüberwachung und die Konformität von Produkten. Weitere Einzelheiten finden Sie auf der Website der Europäischen Kommission:
https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_de

Entwicklung von 41 Normen: 15 horizontale Normen, die allgemein für alle PDE gelten, und 25 vertikale Normen, die auf bestimmte Produkttypen und Risikoklassen zugeschnitten sind. Horizontale Normen befassen sich mit allgemeinen Sicherheitsanforderungen (Typ A) und Anforderungen an die Schwachstellenbehebung (Typ B), während vertikale Normen detaillierte Leitlinien für bestimmte Produkte, z. B. Browser, IoT-Geräte (Typ C), enthalten und beeinflussen, ob Hersteller eine Selbstbewertung vornehmen oder die Einhaltung durch Dritte verlangen können, wobei die sensibelsten Normen unter eingeschränkten Bedingungen entwickelt werden. Eine vollständige Liste der Normen finden Sie auf der Website von CEN/CENELEC unter.[20]

Die Planung für die Bereitstellung dieser Normen sieht vor, dass die Normen des Typs A und des Typs B für den Umgang mit Schwachstellen bis zum 30.08.26, alle Normen des Typs C bis zum 30.10.26 und die verbleibenden Normen des Typs B bis zum 30.10.27 bereitgestellt werden.

Zusätzlich zu den harmonisierten Normen, die die CRA-Konformität direkt unterstützen, werden Hersteller dazu angehalten, bei der Umsetzung der CRA-Anforderungen führende Industrienormen zu verwenden. Bemerkenswerte Beispiele sind in Anhang C aufgeführt.

5.1.2 Gemeinsame Spezifikationen (verabschiedet durch den Durchführungsrechtsakt der Europäischen Kommission) sind detaillierte, praktische Leitlinien der Europäischen Kommission, die Herstellern helfen sollen, bestimmte Cybersicherheitsanforderungen zu erfüllen, wenn keine harmonisierten Normen vorliegen oder wenn Bereiche in einer veröffentlichten harmonisierten Norm nicht ausreichend behandelt werden, und die in solchen Fällen als Ausweichmöglichkeit dienen.

5.1.3 Zertifikate, die im Rahmen eines europäischen Cybersicherheits-Zertifizierungssystems ausgestellt wurden.
Das wichtigste EU-Zertifizierungssystem, das die Einhaltung der CRA unterstützt, ist das EUCC (European Common Criteria). Das EUCC ist ein freiwilliges europaweites Cybersicherheits-Zertifizierungssystem, das die Zertifizierung von IKT-Produkten wie technologischen Komponenten (Chips, Smartcards), Hardware und Software ermöglicht. Aufbauend auf dem seit über zwanzig Jahren bestehenden Bewertungsrahmen SOG-IS Common Criteria dient es als Fortsetzung und Erweiterung (von derzeit 17 EU-Mitgliedstaaten auf alle 27, die es übernehmen werden). Es schlägt zwei Sicherheitsstufen vor, die sich nach dem mit der beabsichtigten Verwendung des Produkts, der Dienstleistung oder des Prozesses verbundenen Risiko in Bezug auf die Wahrscheinlichkeit und die Auswirkungen eines Unfalls richten.
Die Europäische Kommission hat alle Dokumente und Leitlinien im Zusammenhang mit EUCC unter[21] zentralisiert. Die Entscheidung für eine EU-Cybersicherheitszertifizierung als Konformitätsbewertungsverfahren bietet den Vorteil der Konformitätsvermutung mit dem CRA, selbst für Kategorien mit hohem Risiko, und stärkt die Glaubwürdigkeit des Marktes und das Vertrauen der Kunden.

[20] Verfügbar unter: https://www.cencenelec.eu/media/CEN-CENELEC/News/Newsletters/2025/m_606_work_programme_final.pdf
[21] Verfügbar unter: https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_de

Der EU-Cybersicherheitsakt (EU 2019/881) schafft einen gemeinsamen Rahmen für die Zertifizierung der Cybersicherheit in der gesamten EU. Im Rahmen des Cyber Resilience Act (CRA) wird dieser Rahmen besonders wichtig für Produkte mit höheren Risiken, die in Anhang VIII als **wichtig (Klasse II)** oder **kritisch** eingestuft sind. Für diese Produktklassen kann die Zertifizierung als formeller Nachweis für die Erfüllung „erheblicher“ oder „hoher“ Sicherheitsniveaus dienen.

5.2 Mindestanforderungen an Konformitätsbewertungsverfahren

KMU sollten mindestens die im CRA für ihre Produktkategorie festgelegten Mindestanforderungen erfüllen, wie im Dokument „Confirmate D3.1 – Architecture for Automated CRA Conformance Assessment”[22] erläutert**, ODER** ein anderes, anspruchsvolleres Verfahren anwenden. Je anspruchsvoller das gewählte Bewertungsverfahren ist, desto sicherer und vertrauenswürdiger erscheint das PDE auf dem Markt, was einen erheblichen Wettbewerbsvorteil darstellen kann. Wenn das PDE beispielsweise in die Kategorie „Standard“ fällt, ist das minimal erforderliche Verfahren Modul A, aber das KMU kann jedes der anderen, anspruchsvolleren Verfahren unten wählen. Befindet sich ein PDE in der wichtigen Klasse I, kann das herstellende KMU eine Selbstbewertung anhand der harmonisierten Normen für seinen Produkttyp vornehmen, sofern diese verfügbar sind. Sind diese nicht verfügbar, kann das KMU das nächsthöhere Verfahren wählen – Modul B+C oder Modul H. Ist ein PDE in der wichtigen Klasse II aufgeführt, sind mindestens zwei Verfahren erforderlich: „Modul B+C“ oder Modul H, die beide eine Bewertung durch Dritte erfordern.

[22] Verfügbar unter https://confirmate-project.eu/materials/

Die Verfahrensoptionen für bestimmte Produkte sind in der folgenden Tabelle zusammengefasst, wobei jedes Häkchen eine Option für die jeweilige Kategorie darstellt:

Typ/Produktkategorie	Standard	Wichtige Klasse I	Wichtige Klasse II	Kritisch
Selbstbewertung (Modul A – Interne Kontrolle)	✅			
Selbstbewertung anhand der harmonisierten EU-Norm, gemeinsame Spezifikationen (Modul A – Interne Kontrolle)	✅	✅		
CAB-Bewertung der Konstruktion + Selbstbewertung der Produktion (Modul B+C)	✅	✅	✅	
Vollständige CAB-Qualitätssicherung (Modul H)	✅	✅	✅	
EU-Cybersicherheitszertifikat (CSA) auf der Stufe „erheblich“ oder „hoch“	✅	✅	✅	✅

Eine Ausnahme gilt für Open-Source-Produkte: *„Hersteller wichtiger Produkte mit digitalen Elementen, die als freie und quelloffene Software gelten, sollten das interne Kontrollverfahren auf der Grundlage von Modul A anwenden können, sofern sie die technische Dokumentation der Öffentlichkeit zugänglich machen.“* (CRA-Erwägungsgrund 91).

5.3 CE-Kennzeichnung und technische Dokumentation

5.3.1 CE-Kennzeichnung

Die CE-Kennzeichnung ist in der CRA definiert als *„eine Kennzeichnung, durch die ein Hersteller erklärt, dass ein Produkt mit digitalen Elementen und die vom Hersteller festgelegten Verfahren den grundlegenden Cybersicherheitsanforderungen in Anhang I und anderen geltenden Harmonisierungsrechtsvorschriften der Union über ihre Anbringung genügen“.*
Im Allgemeinen ist die CE-Kennzeichnung erforderlich, um zu bestätigen, dass ein Produkt alle geltenden EU-Anforderungen an Cybersicherheit und Sicherheit erfüllt. Im Zusammenhang mit dem CRA sollte die CE-Kennzeichnung erst nach (a) Abschluss des entsprechenden Konformitätsbewertungsverfahrens und (b) Ausarbeitung und Unterzeichnung der EU-Konformitätserklärung angebracht werden.
Die CE-Kennzeichnung unterliegt den allgemeinen Grundsätzen gemäß Artikel 30 der Verordnung (EG) Nr. 765/2008. Die CE-Kennzeichnung sollte sichtbar, lesbar und dauerhaft auf dem Produkt und der Verpackung oder in den Begleitunterlagen (wenn eine physische Kennzeichnung nicht möglich ist) angebracht werden.

Wichtiger Hinweis: *Nicht alle Produkte müssen eine CE-Kennzeichnung tragen. Sie ist nur für die meisten Produkte vorgeschrieben, die unter die Richtlinien nach dem neuen Konzept fallen. Es ist verboten, andere Produkte mit der CE-Kennzeichnung*

zu versehen. Bitte beachten Sie, dass eine CE-Kennzeichnung nicht bedeutet, dass ein Produkt von der EU oder einer anderen Behörde als sicher zugelassen wurde. Sie gibt auch keinen Hinweis auf die Herkunft eines Produkts.[23]

[23] *Siehe vollständigen Text und alle Optionen für das CE-Kennzeichnungsformat auf der Website der Europäischen Kommission: https://single-market-economy.ec.europa.eu/single-market/goods/ce-marking_en*

5.3.2 Technische Dokumentation

Hersteller sind verpflichtet, technische Unterlagen (gemäß Anhang VII der CRA) zu erstellen und aufzubewahren, aus denen die Konformität des Produkts hervorgeht. Dies ist sowohl für die Selbstbewertung als auch für die Bewertung durch Dritte obligatorisch.

Diese Dokumentation muss Folgendes enthalten:

- allgemeine Produktbeschreibung
- eine Beschreibung der Konzeption, Entwicklung und Herstellung des Produkts
- anfängliche und aktualisierte Risikobewertungen
- relevante Informationen, die bei der Festlegung der Unterstützungsdauer berücksichtigt wurden
- eine Liste der harmonisierten Normen, die vollständig oder teilweise auf das Produkt angewendet wurden
- Prüfberichte, Inspektionsergebnisse und angewandte Normen
- Beschreibung des angewandten Konformitätsbewertungsverfahrens
- eine Kopie der EU-Konformitätserklärung
- gegebenenfalls die Stückliste der Software

Für KMU wird in einer Durchführungsverordnung der Kommission, die zum Zeitpunkt der Erstellung dieses Leitfadens noch nicht veröffentlicht war, eine Option für eine vereinfachte Form der technischen Dokumentation zur Verfügung gestellt werden.

5.4 Konformitätserklärung

Die Konformitätserklärung (DoC) ist ein Rechtsdokument, in dem bestätigt wird, dass ein Produkt die geltenden grundlegenden Cybersicherheitsanforderungen gemäß Anhang I der CRA erfüllt. Sie wird vom Hersteller nach erfolgreichem Abschluss der entsprechenden Konformitätsbewertungsverfahren erstellt, muss von einem bevollmächtigten Vertreter unterzeichnet werden und den nationalen Marktüberwachungsbehörden zur Verfügung gestellt werden.

Das DoC sollte enthalten:

- Name und Anschrift des Herstellers
- Produktidentifikation
- eine Erklärung zur Einhaltung der CRA
- eine Liste der relevanten Normen und Konformitätsverfahren
- Verweis auf die EU-Baumusterprüfung (falls zutreffend)
- Unterschrift, Datum und Kontaktdaten der verantwortlichen Person

Der Inhalt der Konformitätserklärung ist in den Anhängen V und VI der CRA aufgeführt.

6. Melde- und Post Market-Verpflichtungen

6.1 Meldepflichten

Gemäß Artikel 14 sind KMU verpflichtet, sowohl „aktiv ausgenutzte Schwachstellen“ als auch „schwere Vorfälle“ zu melden. Diese sind wie folgt definiert:

- Eine aktiv ausgenutzte Schwachstelle ist eine Sicherheitslücke, die bereits genutzt wird oder aktiv für böswillige Angriffe genutzt wird.
- Ein schwerwiegender Vorfall ist ein Ereignis, das die Vertraulichkeit, Integrität oder Verfügbarkeit des Produkts beeinträchtigt, einschließlich der Einschleusung von Malware.

Artikel 14 des CRA beschreibt einen schwerwiegenden Vorfall weiter als einen Vorfall, der (a) die Fähigkeit einer PDE, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit sensibler oder wichtiger Daten oder Funktionen zu schützen, beeinträchtigt oder beeinträchtigen kann, **ODER** (b) zur Einführung oder Ausführung von bösartigem Code in einem PDE oder in den Netzwerk- und Informationssystemen eines Nutzers des Produkts geführt hat oder führen kann.
Die Meldepflichten für diese beiden Arten von Ereignissen unterscheiden sich, wie in den folgenden Abschnitten erläutert. Einzelheiten finden Sie in Artikel 14 des CRA.

Neben der Meldepflicht für aktiv ausgenutzte Schwachstellen und schwerwiegende Vorfälle geht die CRA auch von einer freiwilligen Meldung für alle anderen Vorfälle oder Bedrohungen für die PDE aus. Es gilt das gleiche Verfahren der gleichzeitigen Meldung an CSIRT und ENISA über die einheitliche Meldeplattform.

6.2 Meldeverfahren

Alle obligatorischen Meldungen sind über die künftige einheitliche Meldeplattform[24] an die ENISA und gleichzeitig an das CSIRT der Hauptniederlassung des Herstellers in der EU zu übermitteln. Sobald die einheitliche Meldeplattform (siehe unten) verfügbar ist, erfolgt dies über eine einzige Meldung an die Plattform.

Aktiv ausgenutzte Schwachstellen

Die Meldung aktiv ausgenutzter Schwachstellen erfolgt in drei separaten Schritten:

- Schritt 1: Frühwarnung innerhalb von **24 Stunden** nach Bekanntwerden. Gegebenenfalls sollten in dieser Phase die Mitgliedstaaten identifiziert werden, in denen das Produkt verfügbar gemacht wurde.
- Schritt 2: Erste Meldung der Schwachstelle innerhalb von **72 Stunden** nach Bekanntwerden, einschließlich:
    - allgemeinen Informationen über das Produkt, die Art des Exploits und die betreffende Schwachstelle.
    - alle ergriffenen Korrektur- oder Abhilfemaßnahmen sowie Korrektur- oder Abhilfemaßnahmen, die Nutzer ergreifen können.

[24] Siehe Artikel 16 der CRA: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402847

    - eine Bewertung der Sensibilität der gemeldeten Informationen durch den Hersteller.
- Schritt 3: Abschließender Bericht spätestens **14 Tage** nach Verfügbarkeit einer Korrektur, einschließlich:
    - Beschreibung der Sicherheitslücke, einschließlich ihrer Schwere und Auswirkungen;
    - osweit verfügbar, Informationen über böswillige Akteure, die die Schwachstelle ausgenutzt haben oder ausnutzen;
    - Details zu dem Sicherheitsupdate oder anderen Korrekturmaßnahmen, die zur Behebung der Schwachstelle bereitgestellt wurden.

Schwerwiegende Sicherheitsvorfälle

Die Meldung schwerwiegender Sicherheitsvorfälle erfolgt ebenfalls in drei separaten Schritten, wobei der wesentliche Unterschied im letzten Schritt liegt.

- Schritt 1: Frühwarnung innerhalb von **24 Stunden** nach Bekanntwerden, einschließlich:
    - eine Stellungnahme dazu, ob der Vorfall vermutlich durch rechtswidrige oder böswillige Handlungen verursacht wurde, wobei auch anzugeben ist.
    - Gegebenenfalls die Mitgliedstaaten, in denen das Produkt verfügbar gemacht wurde.
- Schritt 2: Meldung des Vorfalls innerhalb von **72 Stunden** nach Bekanntwerden, einschließlich:
    - die Art des Vorfalls;
    - eine erste Bewertung des Vorfalls;
    - alle ergriffenen Korrektur- oder Abhilfemaßnahmen sowie Korrektur- oder Abhilfemaßnahmen, die Nutzer ergreifen können;
    - eine Bewertung des Herstellers hinsichtlich der Sensibilität der gemeldeten Informationen.
- Schritt 3: Abschlussbericht innerhalb **eines Monats** nach der 72-Stunden-Meldung, einschließlich:
    - detaillierte Beschreibung des Vorfalls, einschließlich seiner Schwere und Auswirkungen;
    - Art der Bedrohung oder die Ursache, die den Vorfall wahrscheinlich ausgelöst hat;
    - angewandte und laufende Abhilfemaßnahmen.

Benachrichtigung der Benutzer

Bei beiden Arten von Vorfällen müssen Hersteller, sobald sie Kenntnis von einer Schwachstelle oder einem Vorfall haben, die betroffenen (und gegebenenfalls alle) Benutzer unverzüglich informieren, einschließlich Empfehlungen zur Risikominderung in einem leicht automatisierbaren, maschinenlesbaren Format. Wenn Hersteller die Benachrichtigung unterlassen, kann das CSIRT einschreiten, um die Benutzer zu informieren.

Freiwillige Meldung

Über ihre Meldepflichten gemäß Artikel 15 hinaus werden die Hersteller dazu angehalten, freiwillig alle Schwachstellen und Bedrohungen zu melden, die die Cybersicherheit eines PDE beeinträchtigen könnten. Entsprechend ist auch die Meldung von Vorfällen, die nicht schwerwiegend sind, freiwillig.

Dieser freiwillige Meldemechanismus könnte eine bewährte Praxis für KMU einführen, die sich indirekt positiv auf den Hersteller und seine Kunden auswirkt, da sie die Sichtbarkeit der Bedrohung erhöht und somit weitere Vorfälle verhindert. Darüber hinaus scheint die freiwillige Meldung die sicherere Option zu sein, wenn es schwierig ist, genau zu beurteilen, ob eine bestimmte Schwachstelle aktiv ausgenutzt wird oder ein Vorfall schwerwiegend ist.

6.3 Zusammenarbeit mit EU- und nationalen Behörden

6.3.1 ENISA und CSIRTs zum Umgang mit Schwachstellen

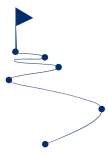
Die Hersteller melden aktiv ausgenutzte Schwachstellen und schwerwiegende Vorfälle gemäß den Bestimmungen in Artikel 14 des Gesetzes an die ENISA und das nationale CSIRT. Die Anforderungen an den Hersteller sind in Abschnitt 5.2 dieser Leitlinien dargelegt.

6.3.2 Nationale Marktüberwachungsbehörden

Die Marktüberwachungsbehörden sind für die Durchsetzung der CRA-Verpflichtungen in jedem Land zuständig. Wie dies für die CRA gilt, wird in Kapitel V des CRA erläutert.

Für Hersteller ergeben sich daraus folgende Verpflichtungen:

- bei Untersuchungen, Audits und Inspektionen zu kooperieren;
- auf Anfrage Unterlagen (z. B. SBOM, Risikobewertungen, technische Unterlagen) vorzulegen;
- die MSA über Verstöße und gegebenenfalls über Korrekturmaßnahmen zu informieren.



7. Schritte zur Umsetzung der CRA für KMU

7.1 Erste Bewertung des Umfangs und der Lücken

Der erste Schritt zur Einhaltung des CRA besteht darin, ein klares Verständnis dafür zu entwickeln, welche Produkte in den Anwendungsbereich der CRA fallen, welche Rolle die

Organisation in Bezug auf die Produkte im Anwendungsbereich spielt und welche Anforderungen die Produkte erfüllen und welche nicht. Dies wird durch eine Bewertung des Umfangs und der Lücken erreicht.

Dieses Dokument dient zusammen mit den vom Confirmate-Projekt bereitgestellten Tools dazu, die erste Analyse zu unterstützen: Umfang, Rollenidentifizierung, Lückenbewertung und Überwachung der Verbesserungen im Laufe der Zeit, wenn die nicht konformen Anforderungen von der Organisation behoben werden. In diesem Sinne sollte die Lückenanalyse als „lebendiges Dokument" betrachtet werden, das regelmäßig aktualisiert werden sollte, um die erzielten Fortschritte widerzuspiegeln. Auf diese Weise spiegelt die Bewertung jederzeit genau wider, wo die Organisation in Bezug auf die Konformität steht.

7.2 Entwicklung eines Umsetzungsplans

Der Umsetzungsplan kann erstellt werden, sobald die erste Lückenbewertung durchgeführt wurde. Wie die Bewertung selbst sollte auch der Plan als ein Dokument betrachtet werden, das sich im Laufe der Zeit weiterentwickelt und die im Verlauf des Umsetzungsprojekts gewonnenen Erkenntnisse berücksichtigt.

Was die Planung betrifft, wird empfohlen, einen „Rolling-Wave"-Ansatz zu verfolgen, bei dem die Aktivitäten für die nächsten drei Monate sehr detailliert geplant und die darüber hinausgehenden Aktivitäten nach bestem Wissen und Gewissen geschätzt werden. Zu detaillierte Pläne, die weit in die Zukunft reichen, können kontraproduktiv sein, da langfristige Aktivitäten in der Regel angepasst werden, um den in früheren Phasen eines Projekts gewonnenen Erkenntnissen Rechnung zu tragen.

In jedem Fall sollte die Durchführung einer Risikobewertung, sofern noch nicht vorhanden, Priorität haben, da die Ergebnisse dieser Bewertung die geplanten und umgesetzten Maßnahmen rechtfertigen und es der Organisation ermöglichen, Risiken so effizient wie möglich zu priorisieren.

Was die kurzfristige Planung betrifft, wird empfohlen, die Aktivitäten einfach zu halten, klare Ergebnisse für jede Aufgabe festzulegen und die für jede einzelne Aktivität vorgesehene Zeit so kurz wie möglich zu halten. Dadurch wird das Problem vermieden, dass Aufgaben immer zu 90 % fertiggestellt sind, aber nie zu 100 % abgeschlossen zu werden.

Nicht zuletzt können KMU die Ressourcen, die speziell zur Unterstützung ihrer Einhaltung der CRA im Rahmen des Programms „Digital Europe" entwickelt wurden, in vollem Umfang nutzen: unsere Confirmate-Projekt-Tools, auf die in Anhang E verwiesen wird, und andere Projekte, die in Anhang F aufgeführt sind, sowie die in Anhang D aufgeführten EU- und nationalen Unterstützungsressourcen für KMU.

7.3 Schulung und Sensibilisierung der Mitarbeitenden

Schulungs- und Sensibilisierungsprogramme sind ein wichtiger Bestandteil des Plans zur Erreichung der Konformität. Obwohl in diesen Leitlinien und den begleitenden Tools alle Anstrengungen unternommen wurden, um die Anforderungen der CRA zu vereinfachen, ist es äußerst wichtig, dass die Mitarbeitenden ein umfassendes Verständnis der CRA und der damit verbundenen Richtlinien entwickeln und aufrechterhalten.

Weitere Leitlinien, Tools und Vorlagen, die KMU bei der Umsetzung wesentlicher Sicherheitsanforderungen und der Einhaltung der Dokumentationsanforderungen verwenden können, sind in den Anhängen aufgeführt. Die Verwendung dieser Ressourcen ist mit Ausnahme der Musterkonformitätserklärung nicht obligatorisch, sollte jedoch im Rahmen eines organisationsweiten Plans in Betracht gezogen werden.

8. Zeitpläne und Übergangsfristen

Die wichtigsten Termine im Zeitplan für die Umsetzung der CRA sind wie folgt:

Datum	Ereignis
11.12.24	Das CRA tritt in Kraft.
11.06.26	Verpflichtungen zur Benachrichtigung von Konformitätsbewertungsstellen gelten[25]
30.08.26	Frist für Normen des Typs A und harmonisierte Normen des Typs B für den Umgang mit Schwachstellen
11.09.26	Meldepflichten für Schwachstellen und Sicherheitsvorfälle treten in Kraft.
30.10.27	Frist für verbleibende harmonisierte Normen des Typs B
11.12.27	Vollständige Anwendung der CRA

[25] Dies ist eine Verpflichtung für die Mitgliedstaaten und nicht für die Hersteller.

Anhang A: Vereinfachte EU-Konformitätserklärung

Hiermit erklärt ... [Name des Herstellers], dass das Produkt mit digitalen Elementen vom Typ ... [Bezeichnung des Produkttyps mit digitalen Elementen] der Verordnung (EU) 2024/2847 (1) entspricht.

Der vollständige Wortlaut der EU-Konformitätserklärung ist unter folgender Internetadresse verfügbar: ...

Anhang B: Vorlage für die Risikobewertung

Die interoperable EU-Risikomanagement-Toolbox der ENISA bietet hierfür eine harmonisierte und von der EU anerkannte Methodik. Sie soll die einheitliche Umsetzung des Risikomanagements in der gesamten EU unterstützen und umfasst ISO/IEC 27005, NIS2 und sektorspezifische Praktiken. Es ist jedoch zu beachten, dass diese Toolbox nicht speziell für die Anforderungen des CRA entwickelt wurde, sondern als allgemeines Werkzeug für viele verschiedene Anwendungsbereiche zu betrachten ist.

Die Toolbox enthält standardisierte Vorlagen und Leitlinien für:

- Identifizierung und Bewertung von Vermögenswerten
- Bedrohungs- und Schwachstellenanalyse
- Risikoschätzung und -bewertung
- Definition von Maßnahmen zur Risikobehandlung und -minderung
- Integration mit den gemäß Anhang I der CRA erforderlichen Sicherheitskontrollen[26]

Es unterstützt sowohl qualitative als auch semiquantitative Bewertungen und ist mit nationalen und internationalen Methoden kompatibel. Die Verwendung dieses Toolkits ermöglicht Konsistenz, Überprüfbarkeit und vollständige Rückverfolgbarkeit von Sicherheitsentscheidungen zur Unterstützung von Konformitätsbewertungen und technischen Dokumentationen gemäß CRA.

[26] Beachten Sie, dass dies keine explizite Zuordnung zu den Kontrollen der CRA darstellt.

Anhang C: Relevante Normen

- ETSI TS 103 701, Anhänge B und C können zur Strukturierung auditfähiger technischer Dokumentationen unter Verwendung von ICS/IXIT-Vorlagen verwendet werden.
- **ISO/IEC 27001** – Informationssicherheits-Managementsystem (ISMS)
- **ISO/IEC 27701** – Datenschutz-Managementsystem (PIMS)
- ETSI EN 303 645 – Grundlegende Sicherheitsanforderungen für das Internet der Dinge für Verbraucher, wobei die Abschnitte 4–5 zur Definition grundlegender Sicherheitsanforderungen verwendet werden können
- **OWASP ASVS** – Standard zur Überprüfung der Anwendungssicherheit
- **CIS-Benchmarks** – Richtlinien für sichere Konfiguration
- **Richtlinien der IoT Security Foundation** – Best Practices für die Sicherheit von IoT-Geräten
- **NIST SP 800-53** – **Sicherheits- und Datenschutzkontrollen für Informationssysteme und Organisationen.**
- **NIST SP 800-37** – Risikomanagement-Framework (RMF), das einen Prozess bereitstellt, der Aktivitäten zum Sicherheits-, Datenschutz- und Cyber-Lieferketten-Risikomanagement in den Systementwicklungslebenszyklus integriert.
- **Das NIST Cybersecurity Framework (CSF)** bietet Leitlinien zum Management von Cybersicherheitsrisiken
- **IEC 62443 / ISA-62443** – Sicherheitsstandards für industrielle Automatisierungs- und Steuerungssysteme
- **ISO 9001** – Qualitätsmanagementsystem
- **CMMC** – Zertifizierung des Cybersicherheits-Reifegradmodells
- **DSGVO** – Datenschutz-Grundverordnung

Anhang D: EU- und nationale Unterstützungsressourcen für KMU

Die Europäische Kommission, die EU-Agentur für Cybersicherheit (ENISA) und das Europäische Kompetenzzentrum für Cybersicherheit (ECCC) veröffentlichen Berichte zum Thema Cybersicherheit, von denen viele Leitlinien enthalten, die für KMU bei der Umsetzung der CRA nützlich sein könnten.

Insbesondere die Leitlinien zur Sicherung des Internets der Dinge (IoT)[27] legen die vollständigen Sicherheitsanforderungen für den gesamten Lebenszyklus fest, einschließlich der Anforderungen und des Designs, der Endnutzung und Wartung sowie der Entsorgung. Die Studie wurde speziell entwickelt, um IoT-Herstellern, Entwicklern, Integratoren und allen an der Lieferkette des IoT beteiligten Akteuren zu helfen, bessere Sicherheitsentscheidungen beim Aufbau, der Bereitstellung oder der Bewertung von IoT-Technologien zu treffen.

Darüber hinaus ist der ENISA-Leitfaden zur Cybersicherheit für KMU eine maßgeschneiderte Anleitung zur Verbesserung der Cybersicherheit kleiner Unternehmen, einschließlich Hersteller.

Auf nationaler Ebene besteht die Aufgabe der nationalen Kompetenzzentren für Cybersicherheit darin, die Exzellenz der Forschung und die Wettbewerbsfähigkeit der Union im Bereich der Cybersicherheit zu fördern. Eine Liste der Zentren wurde vom Europäischen Kompetenzzentrum für Cybersicherheit (ECCC) veröffentlicht.[28]

Zusätzlich zu den Kompetenzzentren haben viele EU-Mitgliedstaaten eine nationale Cybersicherheitsagentur eingerichtet. Während sich die Kompetenzzentren auf Forschung und Innovation konzentrieren, decken die Cybersicherheitszentren in der Regel alle Aspekte der Cybersicherheit ab (auch wenn sich die detaillierten Aufgabenbereiche zwischen den Mitgliedstaaten unterscheiden). Beispiele hierfür sind:

- **Belgien**: CCB – Zentrum für Cybersicherheit Belgien
- **Deutschland**: BSI – Bundesamt für Sicherheit in der Informationstechnik
- **Frankreich**: ANSSI – Agence nationale de la sécurité des systèmes d'information
- **Italien**: ACN – Agenzia per la Cybersicurezza Nazionale
- **Rumänien**: DNSC – Directoratul Național de Securitate Cibernetică

Nicht zuletzt erstellen Industrie- und Berufsverbände Ressourcen, um das Verständnis und die Einhaltung der CRA durch ihre Mitglieder zu unterstützen. Beispiele hierfür sind die Digital SME Alliance, ECSO (auf EU-Ebene) und Agoria.

[27] Verfügbar unter: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things
[28] Verfügbar unter: https://cybersecurity-centre.europa.eu/nccs-0_de

Anhang E: CONFIRMATE-Tools

Nachfolgend finden Sie eine kurze Übersicht über die weiteren Leitfäden, Schulungen, Tools und Dokumentationen, die dieses Dokument begleiten. Alle Projektmaterialien sind unterwww.confirmate-project.eu/materials verfügbar.

Teil 1 Leitlinien und Methoden

Pentesting-Methodik: Entwickeltes und von Fachleuten geprüftes Dokument, das KMU bei der Vorbereitung und Durchführung eines effektiven PDE-Pentests gemäß den Anforderungen des Cyber Resilience Act (CRA) unterstützen soll. Basierend auf Industriestandards soll es einen wesentlichen Leitfaden zusammenfassen und bereitstellen, was erforderlich ist und was als Ergebnis eines Produkt-Pentests zu erwarten ist, unter Berücksichtigung spezifischer Produkte, die in eine Reihe von CRA-Kategorien fallen.

D3.1 – Architektur für die automatisierte CRA-Konformitätsbewertung: detaillierte und umfassende Übersicht über das CONFIRMATE-Framework, in der dessen beabsichtigte Funktionalität und Struktur klar und methodisch dargelegt werden. Das Dokument stellt den vom CRA festgelegten Konformitätsbewertungsprozess vor und definiert ihn klar, sodass den Lesern grundlegende Informationen zu den regulatorischen Anforderungen vermittelt werden. Anschließend wird genau dargestellt, wie Endnutzer während ihres gesamten CRA-Konformitätsbewertungsprozesses mit dem CONFIRMATE-Framework arbeiten und davon profitieren werden.
Im Anschluss an die benutzerorientierte Beschreibung spezifiziert das Ergebnis die vorgesehene Softwarearchitektur und beschreibt wesentliche Elemente wie Schlüsselkomponenten, modulare Unterteilungen und die Interaktionen zwischen diesen Elementen.

D2.2 – Evidenz-Datenmodell: Eine Grundlage für die automatische Erfassung und Bewertung technischer Evidenz über verschiedene Technologien hinweg, die sicherstellt, dass die erforderlichen Informationen effizient erfasst und organisiert werden. Durch die Nutzung maschinenlesbarer Formate erleichtert das Modell die Integration von Evidenz in automatisierte Compliance-Tools, reduziert den manuellen Aufwand für die Dokumentation und verbessert die Genauigkeit von Konformitätsbewertungen. Es ist jedoch zu beachten, dass dieser Ansatz keine vollständige Konformität mit der CRA garantiert, da einige der Anforderungen nicht in automatische Datenerfassungsmethoden übertragbar sind. Das Evidenz-Datenmodell ermöglicht auch die Erstellung entsprechender Metriken, die sich aus den wesentlichen Anforderungen der CRA ableiten, und ist mit diesen abgestimmt. Diese Metriken liefern quantifizierbare Messgrößen für die Konformität.

Teil 2 Open-Source-Tool zur automatisierten Konformitätsbewertung

Confirmate schlägt ein Open-Source-Automatisierungstool vor, das die Konformitätsbewertung der wesentlichen Cybersicherheitsanforderungen der CRA rationalisiert, indem es alle wesentlichen Cybersicherheitsanforderungen und -metriken auflistet, die Sicherheitseinstellungen automatisch mit den CRA-Spezifikationen vergleicht und den

individuellen Handlungsbedarf ermittelt. Seine intuitiven Dashboards und strukturierten Funktionen helfen Unternehmen, schnell zu erkennen, welche wesentlichen Cybersicherheitsanforderungen der CRA bereits umgesetzt wurden und welche noch bewertet oder umgesetzt werden müssen. So sparen sie wertvolle Zeit bei der Konformitätsprüfung und erhalten gleichzeitig klare, umsetzbare Erkenntnisse für die kontinuierliche Einhaltung und Verbesserung der Vorschriften.

Darüber hinaus bieten Dokumentationstools wie das

- D2.2 – Evidence Data Model, das die Automatisierung der Compliance-Überprüfung durch einen strukturierten Ansatz zur Sammlung und Bewertung von Nachweisen ermöglicht.
- D3.1 – Architektur für die automatisierte CRA-Konformitätsbewertung, ein Dokument, das einen detaillierten und umfassenden Überblick über das CONFIRMATE-Framework bietet, dessen beabsichtigte Funktionalität und Struktur umreißt, den Konformitätsbewertungsprozess vorstellt und veranschaulicht, wie Endnutzer mit CONFIRMATE im CRA-Konformitätsbewertungsprozess umgehen und davon profitieren werden.

Teil 3 CONFIRMATE-Schulungen und -Workshops

Die Liste ist ein sich weiterentwickelndes Dokument, das eine Reihe von Schulungen und Workshops enthält, die bis Juli 2026 geplant sind.

CRA-Compliance-Einführung: All you need to know about the EU Cyber Resilience Act (CRA)[29] bietet einen umfassenden Überblick über die wichtigsten Grundsätze und Verpflichtungen des CRA. Das Video erklärt, wie sich die CRA auf Hersteller, Einführer, Händler und Open-Source-Software-Verwalter auswirkt, indem es Rollen und Verantwortlichkeiten, risikobasierte Produktklassifizierungen (Standard, wichtig und kritisch) sowie Sicherheitsanforderungen, CE-Kennzeichnung und Konformitätsbewertungen umreißt. Es behandelt auch wichtige Themen wie die Offenlegung von Schwachstellen, die Meldung von Vorfällen, die Software-Stückliste (SBOM), Durchsetzungsfristen und Strafen bei Nichteinhaltung.

Erläuterung der Pentesting-Methodik: Preparing for a CRA-Aligned Product Pentesting: A Short Training for EU SMEs[30]

Als Teil der Schulungsreihe zur Einhaltung des Cyber Resilience Act (CRA) bietet dieses Modul eine umfassende, schrittweise Anleitung zur Penetrationstest-Methodik für Produkte mit digitalen Elementen. Es richtet sich an Hersteller, KMUs und Cybersicherheitsteams, die die CRA-Anforderungen effektiv und effizient erfüllen möchten. Die Schulung behandelt die fünf wichtigsten Phasen von CRA-konformen Penetrationstests und erklärt, wie Tests gemäß den CRA-Standards geplant, durchgeführt und berichtet werden. Außerdem werden die

[29] verfügbar auf YouTube
[30] verfügbar auf YouTube

Compliance-Anforderungen für Produkte der Klassen „Important Class I“, „Important Class II“ und „Default“ erläutert.

Anhang F: Tools anderer EU-Projekte

Zeitgleich mit CONFIRMATE wurde eine Reihe weiterer EU-Projekte ins Leben gerufen, um KMU bei der Einhaltung der CRA zu unterstützen. Jedes Projekt hat einen anderen Schwerpunkt, stammt aus einer anderen Ländergruppe und schafft ergänzende Ressourcen und Tools. Die Liste der Projekte, die im Zeitraum 2025-2026 laufen und von CyberStandEU[31] zusammengestellt wurden, lautet wie folgt:

1. CRA-AI: Das Projekt CRA-AI entwickelt eine KI-gestützte Plattform, die KMU dabei helfen soll, die Anforderungen des EU-Cyberresilienzgesetzes zu erfüllen und einzuhalten. Dabei werden Cybersicherheitsexperten aus sechs EU-Ländern zusammengebracht.
2. CURIUM: CURIUM entwickelt das Compliance Continuum, eine Reihe von Tools zur Automatisierung und Vereinfachung der Einhaltung des EU-Cyberresilienzgesetzes (CRA). Durch das Angebot von Cybersicherheitsbewertungen, Risikomanagement und Schwachstellentests hilft es KMU, Kosten zu senken, die Zertifizierung zu beschleunigen und das digitale Sicherheitsökosystem Europas zu stärken.
3. OSCRAT: OSCRAT entwickelt kostenlose Open-Source-Tools, um europäischen KMU, politischen Entscheidungsträgern und Industrieverbänden dabei zu helfen, die Anforderungen des Cyber Resilience Act (CRA) zu erfüllen und ihre Cybersicherheitspraktiken zu stärken.
4. OCCTET: OCCTET ist ein von der EU finanziertes Projekt zur Entwicklung eines Open-Source-Toolkits, das KMU dabei unterstützt, die Einhaltung des Cyber Resilience Act (CRA) für Open-Source-Software zu automatisieren. Das Toolkit umfasst eine Compliance-Checkliste, automatisierte Bewertungsinstrumente, eine föderierte Datenbank, Tools zur Abhängigkeitsanalyse und Ressourcen für die Berichterstattung.
5. CYBERFORT: CYBERFORT hilft KMU bei der Erfüllung der Anforderungen des Cyber Resilience Act (CRA), indem es maßgeschneiderte Tools, fachkundige Beratung und Schulungen anbietet. Durch eine offene Plattform und die Zusammenarbeit mit Cybersicherheitsfirmen, Behörden und Branchenakteuren stärkt es die Cyberresilienz und das Bewusstsein in ganz Europa.
6. TRUSTBOOST: TrustBoost ist ein von der EU finanziertes Projekt (Fördervereinbarung Nr. 101158687), das vom Europäischen Kompetenzzentrum für Cybersicherheit unterstützt wird. Seine Aufgabe ist es, die Cybersicherheit, Resilienz und Compliance in der gesamten EU zu stärken, indem es die Zusammenarbeit bei der Zertifizierung und Einhaltung wichtiger EU-Rechtsvorschriften fördert.
7. CRACoWi: CRACoWi (Cyber Resilience Act Compliance Wizard) ist ein EU-Projekt zur Entwicklung eines digitalen Assistenten, der KMU, Herstellern, Händlern und Einführeren dabei hilft, die Standards des Cyber Resilience Act (CRA) zu erfüllen und die Produktsicherheit vom Entwurf bis zur Vermarktung sicherzustellen.
8. CRACY: CRACY (CRA made Easy) hilft europäischen KMU bei der Erfüllung der Anforderungen des Cyber Resilience Act (CRA), indem es die Einhaltung der Vorschriften für Produkte mit digitalen Elementen vereinfacht und bewährte Verfahren sowie sicherere Produkte und Dienstleistungen fördert.

[31] verfügbar unter: https://cyberstand.eu/events/impacting-cra-defining-standards-future

Anhang G: Verhältnis zu anderen EU-Rechtsvorschriften

Obwohl es nicht möglich ist, in diesem Dokument eine vollständige Erörterung der Beziehung zwischen dem CRA und anderen EU-Rechtsvorschriften zu geben, werden im Folgenden einige der wichtigeren Zusammenhänge erwähnt:

1. *New Legislative Framework (EG/2008/765 & EG:2008/768):* Der CRA baut auf dem NLF auf und erweitert den Rahmen im Wesentlichen auf Produkte mit digitalen Elementen. Dies wird in Abschnitt 4.1 dieser Leitlinien ausführlich beschrieben.
2. *Cyber-Resilienz:* Sowohl die NIS2-Richtlinie als auch die DORA-Verordnung zielen darauf ab, die Cyber-Resilienz in der gesamten EU zu verbessern. Sie legen das Cybersicherheits-Risikomanagement und die Meldung von Vorfällen durch Unternehmen in Bezug auf ihre wesentlichen Dienste fest. Die CRA ergänzt diese Initiativen durch die Auferlegung von Sicherheitsanforderungen für Produkte mit digitalen Elementen, die in den EU-Rechtsrahmen für Produkte einfließen.
3. *Die Funkgeräterichtlinie (RED) (Richtlinie 2014/53/EU)* konzentriert sich auf die Sicherheit, elektromagnetische Verträglichkeit und Interoperabilität von Produkten mit Funkausrüstung. Die CRA konzentriert sich auf Cybersicherheit und hat einen breiteren Anwendungsbereich (einschließlich Software, nicht nur IoT). Sie ersetzt den delegierten Rechtsakt der RED für Cybersicherheit.
4. *Die Maschinenverordnung (Verordnung (EU) 2023/1230)* regelt die Gesundheit und Sicherheit bei der Verwendung von Maschinen. Sie ergänzt die CRA, die für digitale Komponenten von Maschinen gilt. Beide Verordnungen gelten gleichzeitig.
5. *EU-DSGVO:* Die CRA baut auf der DSGVO auf und verlangt den Schutz und die Minimierung aller Daten (personenbezogen oder nicht), die von Produkten mit digitalen Elementen verarbeitet werden, die auf dem EU-Markt in Verkehr gebracht werden.
6. *Das KI-Gesetz* (Verordnung (EU) 2024/1689) regelt die Vertrauenswürdigkeit und Sicherheit von (KI-)Systemen. Es gilt für risikoreiche KI-Funktionen, während die CRA für die Cybersicherheit des Produkts selbst gilt. Ein risikoreiches KI-System muss sowohl dem KI-Gesetz als auch den Cybersicherheitsanforderungen der CRA entsprechen.
7. *Das EU-Gesetz über digitale Dienste (DSA) und das Gesetz über digitale Märkte (DMA)* setzen die Rechenschaftspflicht von Plattformen und die Moderation von Inhalten (DSA) sowie die Marktgerechtigkeit für Gatekeeper (DMA) durch. Die CRA überschneidet sich nicht direkt mit diesen Vorschriften, gilt jedoch für die von den Plattformen und Backend-Systemen verwendete Software.
8. *Cybersecurity Act (CSA)* (Verordnung (EU) 2019/881): Die CRA bezieht sich auf Zertifizierungssysteme, die im Rahmen des CSA gemäß den Anforderungen für die Konformitätsbewertung entwickelt wurden (Einzelheiten siehe Abschnitt 4 dieser Leitlinien).