Countdown zum Cyber Resilience Act (CRA)

Ein umfassender Leitfaden zur Erfüllung der CRA-Anforderungen

Inhaltsverzeichnis

Einführung

Der **Cyber Resilience Act (CRA)** verändert die globale Landschaft der Produktkonformität grundlegend, indem er strenge Cybersicherheitsanforderungen für vernetzte Produkte im Rahmen der CE-Kennzeichnung (Conformité Européenne) integriert. Diese Anforderungen können sich potenziell auf jedes Produkt auswirken, unabhängig von dessen Herkunft, sofern es für den Verkauf in der EU bestimmt ist.

Der CRA, offiziell bekannt als Verordnung (EU) 2024/2847, gilt für jedes Produkt mit digitalen Elementen, dessen beabsichtigter Zweck oder vorhersehbare Nutzung eine direkte oder indirekte Datenverbindung, entweder logisch oder physisch, zu einem Netzwerk oder Gerät beinhaltet.

Dieser praxisorientierte Leitfaden von Digi und NXP bietet einen Überblick über die Anforderungen und deren Umsetzung.

Gemäß dieser Verordnung müssen alle Produkte, die in der Lage sind, sich mit einem Gerät oder Netzwerk zu verbinden, definierte Cybersicherheitsanforderungen erfüllen, um eine CE-Kennzeichnung zu erhalten. Diese Kennzeichnung ist eine gesetzliche Voraussetzung für den Verkauf innerhalb der EU. Produkte, die nicht konform sind, dürfen auf dem EU-Markt nicht in Verkehr gebracht werden.

Im Kern ist der CRA eine Antwort auf anhaltende Defizite in der Cybersicherheit. Obwohl viele Hersteller behaupten, dass ihre Produkte „sicher“ sind, gibt es oft keine verlässliche Möglichkeit für Verbraucher oder Unternehmen, diese Behauptungen zu überprüfen oder einen kontinuierlichen Schutz zu gewährleisten. Der CRA schafft einen einheitlichen, verbindlichen Rahmen für ein Mindestmaß an Cybersicherheitskonformität, der den gesamten Produktlebenszyklus abdeckt.

Zu diesem Zweck legt die Verordnung folgendes fest:

- Gemeinsame Anforderungen für die Markteinführung von Produkten oder Software mit digitalen Elementen, um für alle Hersteller einen einheitlichen Ausgangspunkt sicherzustellen.
- Ein einheitliches Cybersicherheits-Framework für die Planung, das Design, die Entwicklung und die Wartung vernetzbarer Produkte.
- Eine Sorgfaltspflicht, die den gesamten Lebenszyklus eines Produkts abdeckt — nicht nur den Zeitpunkt des Verkaufs.
- Dieses Framework soll die Einhaltung der Vorgaben nicht nur für Hersteller von Endprodukten erleichtern, sondern auch für Zulieferer von Hard- und Softwarekomponenten.

Dieser Rahmen soll die Einhaltung der Vorgaben nicht nur für Hersteller von Endprodukten erleichtern, sondern auch für Zulieferer von Hard- und Softwarekomponenten.

Wie bei früherer EU-Gesetzgebung folgen bereits andere Länder dem Beispiel der CRA. So hat beispielsweise die USA im September 2024 das U S Cyber Trust Mark eingeführt. Dieses freiwillige Kennzeichnungsprogramm unter der Aufsicht der Federal Communications Commission (FCC) soll die Entwicklung sicherer vernetzter Produkte fördern.

Die gute Nachricht ist, dass die Einhaltung der CRA-Anforderungen generell hilft, die Konformität Ihrer Produkte mit den Cybersecurity-Bestimmungen anderer Länder und Regionen zu vereinfachen. Noch wichtiger ist jedoch, dass ein gutes Verständnis des CRA potenziell kostspielige Nacharbeiten, Produktrückrufe und negative Berichterstattungen in den Medien vermeidet, die dem Ansehen Ihres Unternehmens schaden können.

Welche Risiken bestehen bei der Nichteinhaltung des CRA?

Die Einhaltung des CRA ist verpflichtend. Wenn ein unter das Gesetz fallendes Produkt keine CE-Kennzeichnung erhält, darf es in der EU rechtlich nicht verkauft werden. Die Aufsichtsbehörden sind befugt, nicht konforme Produkte vom Markt zu nehmen und Rückrufe anzuordnen, was die Marktpräsenz und den Ruf eines Unternehmens erheblich beeinträchtigen kann.

Darüber hinaus können die Behörden Strafen wegen Nichteinhaltung verhängen. Für jeden Verstoß gegen den CRA droht ein Bußgeld von entweder 15 Millionen € oder 2,5 % des weltweiten Jahresumsatzes eines Unternehmens — je nachdem, welcher Betrag höher ist.

Trotz dieser strengen Konsequenzen gibt es noch weit verbreitete Missverständnisse über den CRA. Ein häufiges Missverständnis betrifft den Zeitplan. Viele Hersteller glauben, dass die Verordnung erst 2027 in Kraft tritt, doch der CRA ist bereits in Kraft getreten. Wichtige Fristen für die Einhaltung rücken schnell näher — siehe **“Countdown zur CRA Konformität” auf Seite 5** für Details.

> Viele Hersteller glauben, dass die Verordnung erst 2027 in Kraft tritt, doch der CRA ist bereits in Kraft getreten.
>
> Siehe **“Countdown zur CRA-Konformität ” auf Seite 5** für Details.

Es herrscht auch weiterhin Verwirrung über den Anwendungsbereich der Verordnung — insbesondere darüber, für welche Produkte sie gilt, wer verantwortlich ist und welche Schritte erforderlich sind, um die Konformität aufrechtzuerhalten. Einige der dringendsten Fragen werden im Abschnitt **“Missverständnisse über den Cyber Resilience Act” auf Seite 4** behandelt. Das Verständnis dieser Details ist entscheidend für Hersteller, Einkaufsleiter und Entwicklungsteams.

Darüber hinaus ist eine gründliche Auseinandersetzung mit den Grundlagen des CRA unerlässlich, um sicherzustellen, dass Ihr Unternehmen, Ihre Lieferkette und Ihre Produktentwicklung den Anforderungen dieser wichtigen Verordnung entsprechen.

Missverständnisse über den Cyber Resilience Act (CRA)

Missverständnis	Realität
Der CRA gilt nur für Unternehmen mit Sitz in Europa.	Alle Hersteller, Importeure und Händler, die Produkte auf dem europäischen Markt bereitstellen, müssen den CRA einhalten, unabhängig davon, wo sich ihr Hauptsitz befindet.
Produkte, die bereits auf dem Markt sind, wenn der CRA in Kraft tritt, sind ausgenommen.	Jedes kommerzielle Produkt, ob bereits vorhanden oder nicht, das nach dem 11. Dezember 2027 wesentlich verändert wird, muss die Anforderungen des CRA erfüllen. Außerdem müssen Hersteller die Ausnahme in Artikel 69 “Übergangsbestimmungen” beachten. Die in Artikel 14 festgelegten Pflichten “Meldepflichten der Hersteller” gelten für alle Produkte, die unter diese Verordnung fallen und vor dem 11. Dezember 2027 in Verkehr gebracht werden.
Nur Hersteller sind für die CRA Konformität verantwortlich.	Der CRA gilt für die gesamte Lieferkette, von Herstellern über Importeure und Händler bis hin zu Zulieferern und alle Beteiligten sind für die Einhaltung verantwortlich. Er gilt für Hardware- und Softwareprodukte, sowohl als Endgerät als auch als Komponenten. In diesem Dokument werden diese Gruppen und Personen als “die Verantwortlichen” bezeichnet. Hinweis: Dieses Dokument bezieht sich ausschließlich auf die Verantwortlichkeiten der Hersteller.

Der CRA gilt nur für IT- oder Kommunikationsgeräte.	• Der CRA betrifft die Mehrheit der kommerziellen Produkte mit digitalen Elementen, von IoT-Geräten bis hin zu industriellen Steuerungssystemen.
	• Einige Produkte sind jedoch von den CRA-Anforderungen ausgenommen, da sie bereits durch andere geltende Regelungen abgedeckt sind. Diese sind zum Beispiel:
	  • Medizingeräte und In-vitro Diagnostika
	  • Fahrzeugsysteme und -komponenten
	  • Zivile Luftfahrt
	  • Schiffsausrüstung
	  • Ersatzteile zum Austausch identischer Komponenten in Produkten mit digitalen Elementen
	  • Produkte im Bereich Verteidigung und nationale Sicherheit

Open-Source-Produkte sind vom CRA ausgenommen.	Ob ein Produkt Open-Source-Komponenten enthält, spielt keine Rolle, wenn es ansonsten unter die CRA-Vorgaben fällt.
Der CRA gilt nur für Produkte, die Software enthalten.	Wenn ein kommerzielles Produkt für seine Kernfunktionalität eine Cloud-Plattform oder eine Lösung zur Fern-Datenverarbeitung benötigt, fällt es in den Anwendungsbereich des CRA.
Produkte, die die meiste Zeit offline sind, müssen nicht CRA-konform sein.	Jedes Produkt mit digitalen Elementen, das auch nur potenziell eine Datenverbindung zu einem Gerät oder Netzwerk herstellen kann, muss den CRA Anforderungen entsprechen.
Produkte müssen nur einmal getestet oder zertifiziert werden.	Der CRA schreibt die kontinuierliche Wartung, Konformität und Einhaltung während des gesamten Produkt-Lebenszyklus vor, nicht nur beim Markteintritt.

Grundlagen des CRA

Im Gegensatz zu früheren Regularien führt der CRA konkrete technische Anforderungen, klare Pflichten und definierte Fristen ein — und schafft damit Verantwortlichkeit in der gesamten Lieferkette. Diese neuen Vorschriften basieren auf sechs grundlegenden Säulen:

- ✓ **Strikte Cybersicherheit:** Der CRA legt hohe Sicherheitsanforderungen an Design, Entwicklung, Wartung und Unterstützung nach dem Inverkehrbringen fest. Hersteller müssen ihre Produkte auf Schwachstellen prüfen, diese proaktiv beheben und regelmäßige Updates bereitstellen.
- ✓ **Konformitätsbewertungen:** Produkte müssen vor dem Eintritt in den EU-Markt einer detaillierten Bewertung unterzogen werden, um die Einhaltung der grundlegenden Cybersicherheitsanforderungen nachzuweisen.
- ✓ **Frühzeitige Meldung von Schwachstellen und Vorfällen:** Jede aktiv ausgenutzte Schwachstelle und jeder schwerwiegende Sicherheitsvorfall muss innerhalb von 24 Stunden nach Entdeckung den zuständigen Behörden gemeldet werden, um eine schnelle Reaktion zu ermöglichen.
- ✓ **Produktklassifizierung:** Produkte werden nach Cybersicherheitsrisiko — standard, wichtig, kritisch — eingestuft, mit spezifischen Konformitätsbewertungsverfahren, um angemessene Sicherheitsprüfungen zu gewährleisten.
- ✓ **Überwachung und Audits:** Konformität muss während des gesamten Produktlebenszyklus durch aktive Aufsicht und Audits sichergestellt werden, nicht nur beim Markteintritt.
- ✓ **Transparent und Kommunikation:** HERSTELLER müssen den Nutzern und Behörden klare und aktuelle Informationen über Sicherheitsfunktionen, Schwachstellen und ergriffene Maßnahmen zur Behebung bereitstellen.

Artikel 13, Absatz 19: “Die Hersteller stellen sicher, dass das Enddatum des in Absatz 8 genannten Unterstützungszeitraums, zum Zeitpunkt des Kaufs in leicht zugänglicher Weise und sofern zutreffend auf dem Produkt mit digitalen Elementen, seiner Verpackung oder mit digitalen Mitteln klar und verständlich angegeben wird, wobei mindestens der Monat und das Jahr anzugeben sind.

Sofern dies angesichts der Art des Produkts mit digitalen Elementen technisch machbar ist, zeigen die Hersteller den Nutzern eine Mitteilung an, um sie darüber zu unterrichten, dass das Ende des Unterstützungszeitraums abgelaufen ist.

Zusammen schaffen diese Säulen einen standardisierten Ansatz für Cybersicherheit, der sicherstellt, dass vernetzbare Produkte sowohl vor der Bereitstellung an Endnutzer als auch während ihres gesamten Lebenszyklus wesentliche Cybersicherheitsanforderungen erfüllen.

Hersteller müssen umgehend mit der Implementierung der notwendigen Maßnahmen beginnen um die Einhaltung innerhalb der vorgeschriebenen Fristen sicherzustellen.

Countdown zur CRA-Konformität

Als Teil der EU-Cybersicherheitsstrategie von 2020 wurde der CRA entwickelt, um das **NIS2 Framework**. zu ergänzen. Das Gesetz wurde am 23. Oktober 2024 offiziell vom Europäischen Parlament und dem Rat der Europäischen Union unterzeichnet und am **20. November 2024 veröffentlicht**.

11. Dezember 2024

Der CRA wird offiziell in die EU-Gesetzgebung aufgenommen, mit einer Übergangsfrist, bevor die vollständige Einhaltung verpflichtend wird.

11. Juni 2026

Die für die Überprüfung der CRA-Konformität zuständigen Konformitätsbewertungsstellen nehmen ihre Arbeit auf, wie in Kapitel IV, Artikel 35-51 beschrieben.

Organisationen sollten sich frühzeitig mit den Verfahren zur Konformitätsbewertung vertraut machen und prüfen, ob ihre Produktkategorie eine formale Zusammenarbeit mit einer Konformitätsbewertungsstelle erfordert oder ob eine freiwillige Zusammenarbeit sinnvoll ist, um die Konformität-Bemühungen vor der Frist 2027 zu unterstützen.

11. September 2026

Hersteller sind nun verpflichtet, aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle in den betroffenen Produkten innerhalb von 24 Stunden nach deren Entdeckung sowohl an das zuständige Computer Security Incident Response Team (CSIRT – siehe https://csirtsnetwork.eu/) als auch an die EU-Agentur für Cybersicherheit (ENISA) zu melden, wie in Artikel 14 festgelegt.

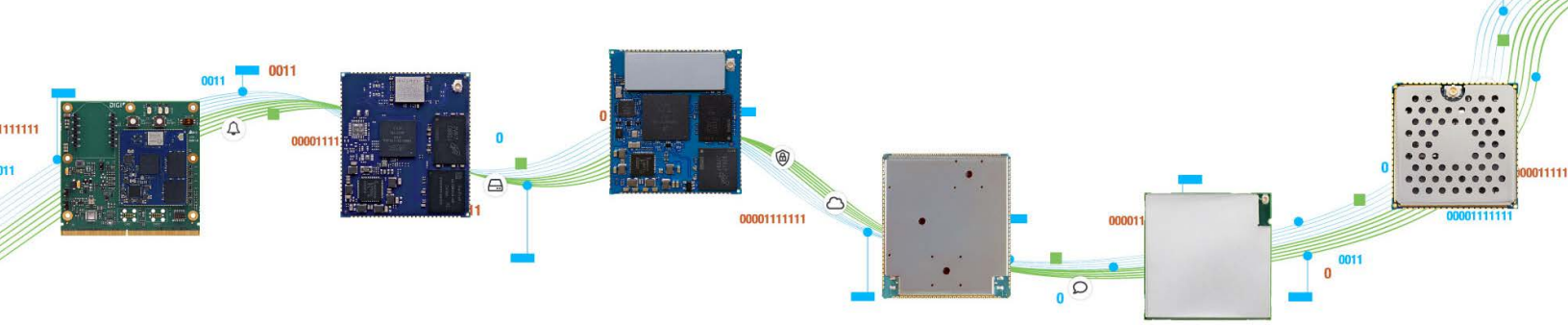
11. Dezember 2027

Der Cyber Resiliance Act tritt offiziell in Kraft. Ab diesem Datum müssen alle betroffenen Produkte eine CE-Kennzeichnung tragen, um in der EU verkauft werden zu dürfen.

Zentrale Anforderungen für die Konformität (Anhang I)

Der CRA schreibt Cybersicherheits-Konformität für Produkte “von der Wiege bis zur Bahre” vor und verlangt sowohl ein sicheres Produktdesign und Produktentwicklung als auch einen kontinuierlichen Schutz über den gesamten Produktlebenszyklus hinweg. Das bedeutet, dass Cybersicherheit bereits in den frühesten Entwicklungsphasen berücksichtigt werden muss und weit über die Produkteinführung hinaus bestehen bleibt. (**Siehe Abschnitt Supportzeitraum auf Seite 7 für weitere Informationen.**)

Um dieses Ziel zu unterstützen, legt Anhang I des CRA zwei Kategorien von Cybersicherheitsanforderungen fest: Teil I konzentriert sich auf die Eigenschaften von Produkten mit digitalen Elementen und Teil II legt Regeln für den Umgang mit Schwachstellen und Lifecycle-Management fest.



Teil I: Produktbezogene Cybersicherheitsanforderungen

Während der Produktentwicklung müssen Unternehmen eine umfassende Cybersicherheits-Risikobewertung durchführen und ein angemessenes Schutzniveau in Bezug auf potenzielle Risiken sicherstellen (Anhang I, Teil I.1). Auf dieser Grundlage müssen Produkte mit digitalen Elementen:

- Zum Zeitpunkt der Markteinführung frei von bekannten ausnutzbaren Schwachstellen sein (Anhang I, Teil I.2(b))
- Mit einer “Secure-by-default” Konfiguration ausgeliefert werden (Anhang I, Teil I.2(b))
- Sicherstellen, dass Schwachstellen durch Sicherheitsupdates behoben werden können, wobei Updates automatisch und standardmäßig aktiviert sein sollen (Anhang I, Teil I.2(c))
- Vor unbefugtem Zugriff durch geeignete Authentifizierungs-, Identitäts- oder Zugriffsverwaltungssysteme geschützt sein (Anhang I, Teil I.2(d))
- Die Vertraulichkeit von Daten schützen, z.B. durch Verschlüsselung gespeicherter oder übertragener Daten mit modernen Mechanismen (Anhang I, Teil I.2(e))
- Die Integrität von gespeicherten, übertragenen oder verarbeiteten Daten, Befehlen, Programmen und Konfigurationen gegen Manipulation schützen und Datenbeschädigungen melden (Anhang I, Teil I.2(f))
- Nur Daten verarbeiten, die für den vorgesehenen Zweck unbedingt erforderlich sind (Anhang I, Teil I.2(g))
- Wesentliche Funktionen beinhalten, die vor Denial-of-Service (DoS) Attacken schützen (Anhang I, Teil I.2(h))
- Potenzielle Auswirkungen auf Dienste anderer Geräte oder Netzwerke, die durch das Produkt oder verbundene Geräte entstehen, minimieren (Anhang I, Teil I.2(i))
- Angriffsflächen, einschließlich externer Schnittstellen, begrenzen (Anhang I, Teil I.2(j))
- Mechanismen zur Ausnutzungsminderung implementieren, um die Auswirkungen von Sicherheitsvorfällen zu reduzieren (Anhang I, Teil I.2(k))
- Sicherheitsrelevante Informationen bereitstellen, indem interne Aktivitäten wie der Zugriff auf oder die Änderung von Daten, Diensten oder Funktionen überwacht und protokolliert werden, gleichzeitig muss den Nutzern die Möglichkeit gegeben werden, dies abzulehnen (Anhang I, Teil I.2(l))
- Sicherstellen, dass auf Wunsch der Nutzer alle Daten und Einstellungen sicher gelöscht oder auf andere Produkte übertragen werden können (Anhang I, Teil l.2(m))

Teil II: Anforderungen zum Umgang mit Schwachstellen

Sichere Produktentwicklung allein ist nicht ausreichend. Der CRA definiert auch Anforderungen für das Management und die Behebung von Schwachstellen. Hersteller müssen alle Schwachstellen und Komponenten eines Produkts identifizieren und dokumentieren. Dazu gehört die Pflege von aktuellen, maschinenlesbaren Software Bill of Materials (SBOM), die mindestens die Top-Level-Abhängigkeiten eines Produkts auflistet (Anhang I, Teil II.1). Der CRA schreibt das Erstellen einer SBOM vor, sie muss jedoch nicht veröffentlicht werden.

Darüber hinaus müssen Hersteller zudem

- Schwachstellen unverzüglich beheben, indem sie Sicherheitsupdates bereitstellen (Anhang I, Teil ll.2)
- Effektive und regelmäßige Tests und Überprüfungen der Produktsicherheit durchführen (Anhang I, Teil II.3)
- Informationen über behobene Schwachstellen weitergeben und öffentlich bekannt machen (Anhang I, Teil II.4)
- Eine Richtlinie für koordinierte Schwachstellenmeldung einführen und durchsetzen (Anhang I, Teil II.5)
- Eine Kontaktadresse für die Meldung entdeckter Schwachstellen bereitstellen (Anhang I, Teil II.6)
- Mechanismen zur sicheren Verteilung von Updates implementieren, um sicherzustellen, dass Schwachstellen zeitnah behoben oder abgeschwächt werden (Anhang I, Teil II.7)
- Sicherheitsupdates unverzüglich, kostenlos und mit Hinweisen, die relevante Informationen enthalten, für die Benutzer bereitstellen. (Anhang I, Teil II.8)

Diese Verfahren im Umgang mit Schwachstellen sollen sicherstellen, dass Produkte auch lange nach ihrer ersten Markteinführung geschützt und konform bleiben, durch koordinierte Maßnahmen über den gesamten Supportzeitraum eines Produkts und darüber hinaus.

Zentrale Verpflichtungen (Artikel 13 und 14)

Zusätzlich zu den Cybersicherheitsanforderungen für Produktdesign, -entwicklung, -produktion und -wartung legt der CRA mehrere zentrale Pflichten für Hersteller fest. (Hinweis: Einige dieser Pflichten gelten auch für andere verantwortliche Parteien in der Lieferkette. Dieses Dokument konzentriert sich jedoch ausschließlich auf die Pflichten der Hersteller.) Diese Pflichten sind in den Artikeln 13 und 14 des CRA "Pflichten der Hersteller" und "Meldepflichten der Hersteller" definiert. Dort sind die Verfahren beschrieben, die befolgt werden müssen, um sicherzustellen, dass Produkte die in Anhang I, Teile I und II festgelegten grundlegenden Cybersicherheitsanforderungen erfüllen.

CRA-Artikel 13: Pflichten der Hersteller

Artikel 13 legt die Pflichten der Hersteller fest. Diese Pflichten lassen sich in drei Phasen einteilen: Design und Entwicklung, Supportzeitraum und Verfügbarkeit von Sicherheitsupdates.

Design und Entwicklung

In der ersten Phase, Design und Entwicklung, schreibt die Verordnung eine Reihe von Pflichten vor:

- Sicherstellen, dass das Produkt in Übereinstimmung mit den grundlegenden Cybersicherheitsanforderungen gemäß Anhang I, Teil I entwickelt, entworfen und produziert wurde.
- Durchführung einer Cybersicherheits-Risikobewertung für das Produkt, die während des gesamten Supportzeitraums dokumentiert und aktualisiert wird.
- Die Risikobewertung muss den vorgesehenen Zweck des Produkts, mögliche Nutzungen, Nutzungsbedingungen (z.B. die Betriebsumgebung oder zu schützende Werte) sowie den Supportzeitraum berücksichtigen. Die Risikobewertung muss aufzeigen, ob die in Anhang I, Teile I und II festgelegten grundlegenden Cybersicherheitsanforderungen für das betreffende Produkt gelten und wie diese Anforderungen praktisch umgesetzt werden.
- Die Ergebnisse der Risikobewertung müssen in die technische Dokumentation des Produkts (Artikel 31 und Anhang VII) aufgenommen werden, einschließlich einer klaren Begründung für das Weglassen einzelner grundlegender Cybersicherheitsanforderungen. Diese Ergebnisse müssen die Entscheidungen und Maßnahmen in allen Phasen; Planung, Design, Entwicklung, Produktion, Lieferung und Wartung leiten.
- Es wird besonders betont, dass Hersteller die gebotene Sorgfalt walten lassen müssen, wenn sie Drittkomponenten integrieren, damit diese die Produktsicherheit nicht beeinträchtigen. Dies gilt auch für freie und Open-Source-Softwarekomponenten, die nicht kommerziell auf dem Markt erhältlich sind.
- Hersteller müssen die von ihnen gewählten Verfahren zur Konformitätsbewertung gemäß Artikel 32 durchführen oder durchführen lassen.
- Sobald ein Hersteller nachgewiesen hat, dass sein Produkt die grundlegenden Cybersicherheitsanforderungen aus Anhang I, Teil I und II erfüllt, muss er gemäß Artikel 28 die EU-Konformitätserklärung erstellen und gemäß Artikel 30 die CE-Kennzeichnung anbringen.

> Artikel 13, Absätze 5, 6 und 8 legen fest, dass Hersteller bei der Integration von Drittkomponenten die gebotene Sorgfalt walten lassen müssen, damit diese Komponenten die Produktsicherheit nicht beeinträchtigen. Dies gilt ausdrücklich auch für die Produktintegration von Open-Source-Softwarekomponenten, die ohne Gewinnerzielungsabsicht erhältlich sind.

Supportzeitraum

Kommen wir nun zur nächsten Phase: dem Supportzeitraum.

- Das Produkt wurde bereits in Verkehr gebracht und der Supportzeitraum beginnt — währenddessen ist der Hersteller verpflichtet sicherzustellen, dass die Schwachstellen des Produkts wirksam und im Einklang mit den in Anhang I, Teil II formulierten grundlegenden Cybersicherheitsanforderungen behandelt werden.
- Hersteller müssen den Supportzeitraum so festlegen, dass er die erwartete Nutzungsdauer des Produkts widerspiegelt, wobei dieser in der Regel mindestens fünf Jahre beträgt. Bei der Festlegung des Supportzeitraums müssen sie unter anderem die Erwartungen der Nutzer, die Art des Produkts, dessen Verwendungszweck, Supportzeiträume für Produkte mit ähnlicher Funktionalität anderer Hersteller, die Verfügbarkeit der Betriebsumgebung sowie die Supportzeiträume integrierter Komponenten, die die Hauptfunktionen bereitstellen und von Dritten bezogen werden, berücksichtigen.
- Hersteller müssen in der technischen Dokumentation gemäß Anhang VII die Informationen aufnehmen, die bei der Festlegung des Supportzeitraums des Produkts berücksichtigt wurden.

- Zu beachten ist, dass der Supportzeitraum mit dem Inverkehrbringen eines Produkts beginnt. Das Enddatum des Supportzeitraums ergibt sich aus dem letzten Verkauf des Produkts auf dem Markt plus fünf Jahre. Somit beträgt der Supportzeitraum zwar weiterhin fünf Jahre, aber sein Ende verschiebt sich dynamisch, solange das Produkt weiter auf den Markt gebracht wird. Der Countdown beginnt in der Praxis mit dem Verkauf der letzten Charge des Produkts. Der Supportzeitraum läuft also bis zum Ende des Produktlebenszyklus bzw. bis zur letzten Lieferung an Kunden auf dem EU-Markt, plus fünf Jahre.

- Wichtig ist, dass die Hersteller die volle Verantwortung für die Identifizierung, Bearbeitung und Offenlegung von Schwachstellen aller Komponenten tragen, auch derjenigen, die von Drittanbietern stammen. Wenn Schwachstellen in Drittkomponenten behoben werden, müssen die Hersteller dem Komponentenhersteller die relevanten Unterlagen oder den Code zur Verfügung stellen.

- Artikel 13 verlangt außerdem, dass Hersteller alle relevanten Aspekte in Bezug auf die Produktsicherheit dokumentieren, einschließlich aller bekannten Schwachstellen sowie relevanter Informationen, die von Dritten bereitgestellt werden. Hersteller müssen umfassende Aufzeichnungen über die Cybersicherheitselemente ihrer Produkte führen, wobei die Dokumentation spezifisch auf das jeweilige Risikoprofil des Produkts zugeschnitten sein muss.

- Darüber hinaus müssen Hersteller geeignete Richtlinien und Verfahren einführen, um Berichte über Schwachstellen von Dritten entgegenzunehmen, zu bearbeiten und darauf zu reagieren. Dies schafft einen effektiven Rückkopplungsprozess, der die kontinuierliche Verbesserung der Sicherheit unterstützt.

- Hersteller müssen die technische Dokumentation und die EU-Konformitätserklärung für mindestens zehn Jahre nach der Produkteinführung oder für die Dauer des Supportzeitraums, je nachdem, welcher Zeitraum länger ist, den Marktüberwachungsbehörden zur Verfügung halten.

- Ebenso müssen sie die Informationen und Anweisungen für den Benutzer (Anhang II) für mindestens zehn Jahre nach dem Inverkehrbringen oder für die Dauer des Supportzeitraums, je nachdem, welcher Zeitraum länger ist, für Benutzer und Marktüberwachungsbehörden zugänglich halten.

- Während des Supportzeitraums müssen Hersteller, sobald sie feststellen, dass ihr Produkt oder ihre Prozesse nicht den grundlegenden Cybersicherheitsanforderungen gemäß Anhang I entsprechen, unverzüglich Korrekturmaßnahmen ergreifen oder das Produkt zurückziehen bzw. zurückrufen.

- Hersteller müssen auf Anfrage SBOMs den Marktüberwachungsbehörden zur Verfügung stellen, um EU weite Analysen von Softwareabhängigkeiten zu ermöglichen, insbesondere für freie und Open-Source-Komponenten in bestimmten Produktkategorien.

Der Supportzeitraum für ein Produkt beginnt ab dem Zeitpunkt, an dem das Produkt in Verkehr gebracht wird

Er endet fünf Jahre nach dem letzten Verkauf oder der letzten Auslieferung des Produkts in der EU.

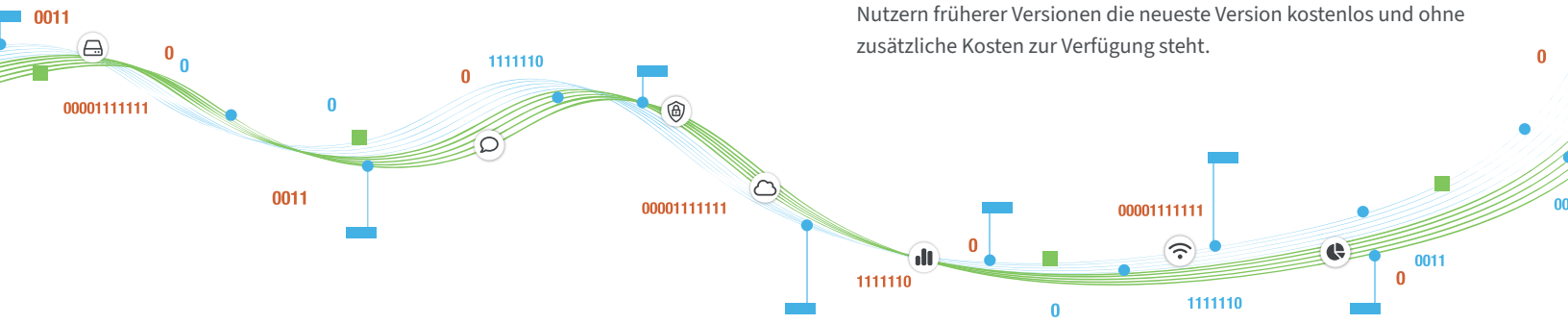
Der Fünfjahreszeitraum beginnt also erst, wenn das Produkt nicht mehr auf dem Markt bereitgestellt wird — das bedeutet, dass sich der Supportzeitraum so lange verlängert, wie die Verkäufe oder Auslieferungen stattfinden.

Verfügbarkeit von Sicherheitsupdates

Abschließend die Verfügbarkeit von Sicherheits updates:

- Hersteller müssen sicherstellen, dass jedes Sicherheitsupdate gemäß Anhang I, Teil II, Punkt 8, das während des Supportzeitraums für die Nutzer bereitgestellt wurde, nach seiner Veröffentlichung für einen Zeitraum von mindestens zehn Jahren oder für den Rest des Supportzeitraums, je nachdem, welcher Zeitraum länger ist, verfügbar bleibt.

- Hersteller können die Einhaltung der grundlegenden Cybersicherheitsanforderung gemäß Anhang I, Teil II, Punkt (2) auf die jeweils zuletzt veröffentlichte Version beschränken, sofern Nutzern früherer Versionen die neueste Version kostenlos und ohne zusätzliche Kosten zur Verfügung steht.



Meldepflichten der Hersteller (Artikel 14)

Ein Hersteller muss aktiv ausgenutzte Schwachstellen und schwerwiegende Vorfälle **innerhalb von 24 Stunden nach deren Entdeckung** melden. Eine aktiv ausgenutzte Schwachstelle ist eine bekannte Schwachstelle, die nachweislich von Angreifern genutzt wird, um Systeme zu kompromittieren. Ein schwerwiegender Vorfall ist ein Ereignis, das schwerwiegende Folgen für das Produkt, seine Nutzer oder verbundene Systeme haben kann — etwa Ausfälle, Sicherheitsverletzungen oder Datenlecks.

In beiden Fällen muss eine Frühwarnmeldung gleichzeitig an die ENISA und an das in jedem Mitgliedstaat benannte CSIRT als Koordinator übermittelt werden. Die Meldung muss angeben, in welchen Mitgliedstaaten das Produkt verfügbar gemacht wurde. Bei schwerwiegenden Vorfällen muss diese Meldung zusätzlich enthalten, ob der Vorfall vermutlich auf illegale oder böswillige Handlungen zurückzuführen ist. Die Meldung erfolgt über eine von ENISA eingerichtete Plattform (Artikel 16).

Der Hersteller ist außerdem verpflichtet, innerhalb von 72 Stunden eine weitere Meldung herauszugeben, die folgendes enthält:

- Allgemeine Informationen über die Schwachstelle oder den Vorfall
- Bisher ergriffene Maßnahmen zur Behebung oder Korrektur
- Hinweise für Nutzer, was sie tun können, um Schäden zu mindern
- Eine erste Einschätzung des Vorfalls
- Die Bewertung des Herstellers, wie sensibel oder vertraulich die gemeldeten Informationen sind

Schließlich muss der Hersteller einen Abschlussbericht sowohl für aktiv ausgenutzte Schwachstellen als auch für schwerwiegende Vorfälle einreichen.

Im Falle von aktiv ausgenutzten Schwachstellen muss ein Abschlussbericht spätestens 14 Tage nach Verfügbarkeit einer Korrektur- oder Abhilfemaßnahme eingereicht werden, der mindestens Folgendes enthalten muss:

- Beschreibung der Schwachstelle, einschließlich ihrer Schwere und Folgen
- Informationen über böswillige Akteure, die die Schwachstelle genutzt haben oder ausnutzen
- Details zum Sicherheitsupdate oder zu anderen verfügbaren Korrekturmaßnahmen

Für schwerwiegende Vorfälle muss ein Abschlussbericht innerhalb eines Monats nach Abgabe der 72-Stunden-Meldung des Vorfalls eingereicht werden, der mindestens Folgendes enthalten muss:

- Detaillierte Beschreibung des Vorfalls, einschließlich seiner Schwere und Auswirkungen
- Art der Bedrohung oder Grundursache, die den Vorfall wahrscheinlich ausgelöst hat
- Umgesetzte und laufende Abhilfemaßnahmem

Wichtige Hinweise zu Konformität und Product Lifecycle

Jedes betroffene Produkt auf dem EU-Markt muss die CRA-Meldepflichten einhalten, einschließlich der Produkte, die vor dem 11. Dezember 2027 kommerziell verfügbar waren. Diese Anforderungen gelten für den gesamten Lebenszyklus aller Produkte mit CE-Kennzeichnung.

Daher müssen Entwicklerteams kontinuierlich potenzielle Schwachstellen in ihren Produkten überwachen und analysieren, diese ordnungsgemäß dokumentieren und an ENISA und CSIRT melden. Für alle identifizierten Schwachstellen müssen die Entwickler Patches erstellen oder beschaffen und diese zeitnah anwenden. Dies bedeutet, dass Hersteller die Möglichkeit integrieren müssen, jedes vernetzbare Gerät über die gesamte Lebensdauer des Produkts zu erreichen und zu aktualisieren, um die Konformität aufrechtzuerhalten.

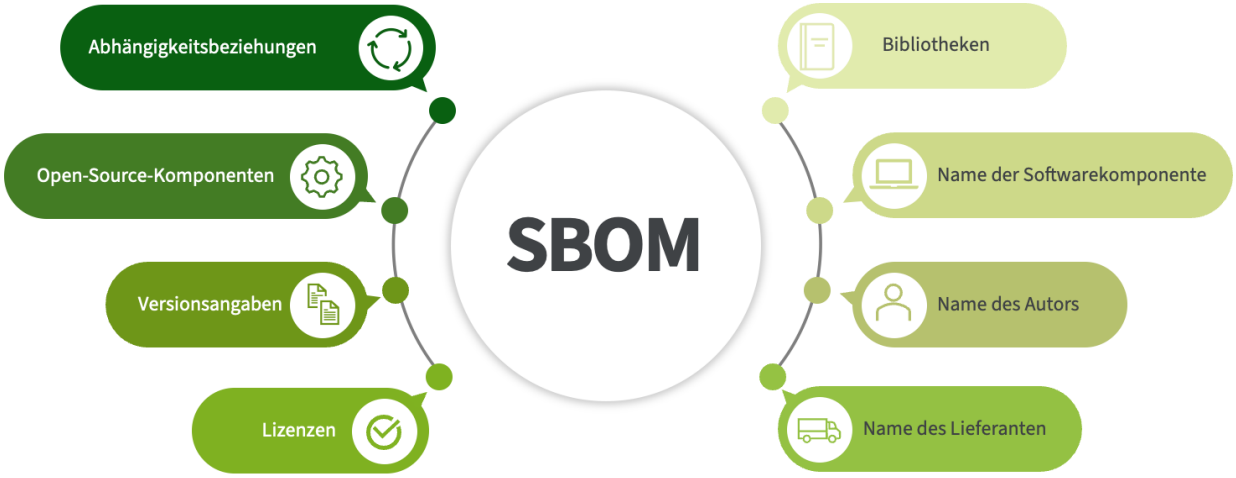
Siehe **Digi's End-to-End Support für CRA Konformität auf Seite 13** um zu erfahren, wie Digi-Lösungen diese Anforderungen unterstützen.

Anforderungen an technische Dokumentationen

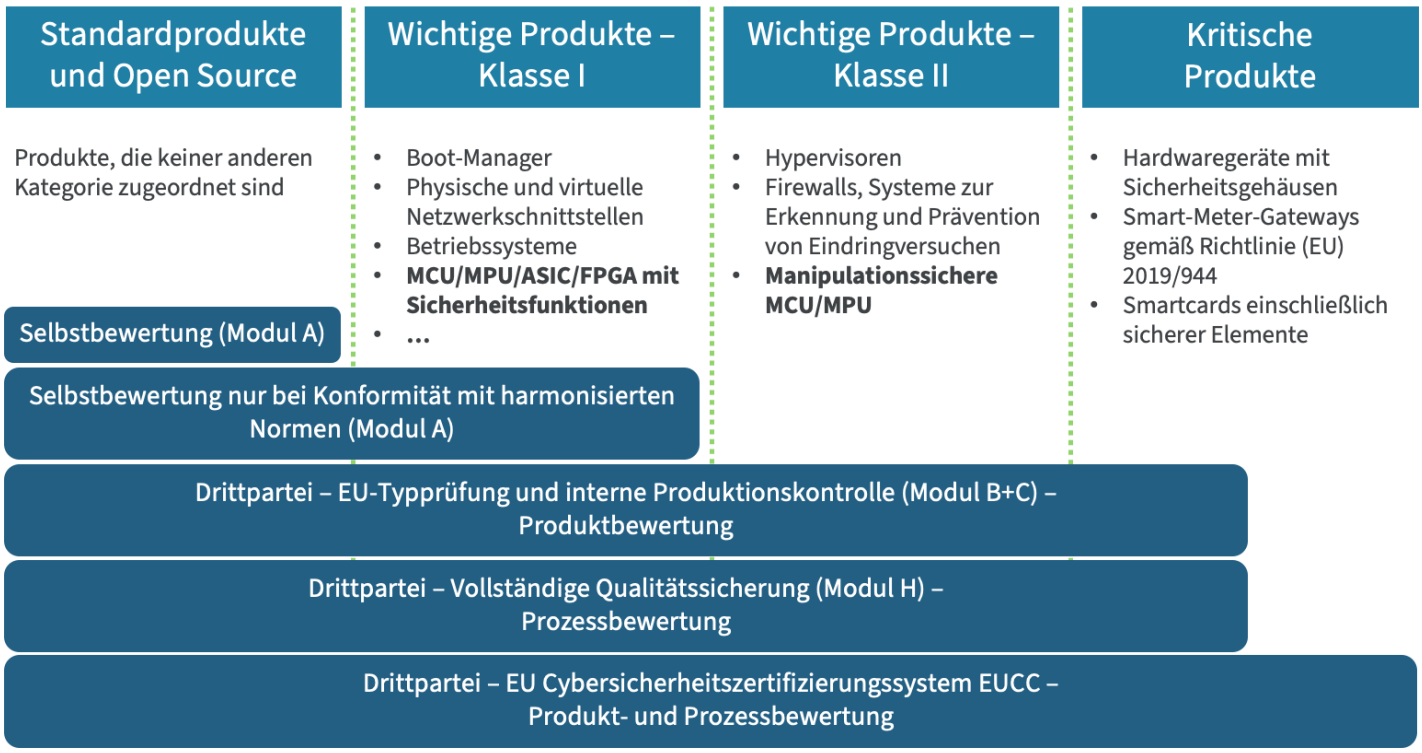
Wie in Artikel 31 erwähnt und in Anhang VII des CRA beschrieben, sind Hersteller verpflichtet, eine Dokumentation zu führen, die Folgendes umfasst:

- Eine allgemeine Beschreibung ihres Produkts, einschließlich des vorgesehenen Zwecks, Informationen zur Software Versionierung, Bilder, die die äußeren Merkmale und Kennzeichnungen sowie das interne Layout zeigen, sowie Benutzerinformationen und Anweisungen gemäß Anhang II
- Angaben zu Design-, Entwicklungs-, Produktions- und Schwachstellenmanagement-Prozessen
- Informationen zum Produktdesign und zur Entwicklung: Zeichnungen/Schemata und eine Beschreibung der Systemarchitektur, die erklärt, wie die Softwarekomponenten zusammenarbeiten und in die Gesamtverarbeitung integriert werden
- Spezifikationen zu den Prozessen des Umgangs mit Schwachstellen, einschließlich der Software-Stückliste (SBOM), der Richtlinie für koordinierte Schwachstellenmeldung, einer Kontaktadresse für Schwachstellenmeldungen und eine Beschreibung der gewählten Lösungen für die sichere Bereitstellung von Updates
- Informationen zu Produktions- und Überwachungsprozessen sowie zur Validierung dieser Prozesse
- Die in Artikel 13 erwähnte Cybersicherheits-Risikobewertung, einschließlich der Darstellung, wie die in Anhang I, Teil I formulierten grundlegenden Cybersicherheitsanforderungen anwendbar sind
- Information darüber, wie der Hersteller gemäß Artikel 13(8) den Supportzeitraum seines Produkts bestimmt hat
- Alle von der EU veröffentlichten harmonisierten Normen, die vollständig oder teilweise auf das Produkt anwendbar sind, einschließlich Cybersicherheits-Zertifizierungsschemata und gemeinsamer Spezifikationen
- Prüfberichte der Tests, die zur Überprüfung der Konformität des Produkts und der Prozesse zum Umgang mit Schwachstellen mit den geltenden grundlegenden Cybersicherheitsanforderungen durchgeführt wurden
- Eine Kopie der EU-Konformitätserklärung des Produkts und eine SBOM, falls zutreffend, auf Anfrage einer Marktüberwachungsbehörde

Zu den Anforderungen an die technische Dokumentation gehören Produktbeschreibungen, Prozesse zum Umgang mit Schwachstellen, Risikobewertungen und SBOMs — diese müssen für mindestens zehn Jahre den Marktüberwachungsbehörden zur Verfügung stehen.



Produktkategorien und Konformitätsbewertungsverfahren



Konformitätsbewertungsverfahren (Artikel 32)

Gemäß Artikel 32 müssen alle Produkte, die in den Geltungsbereich des CRA fallen, einer Konformitätsbewertung unterzogen werden, um die Einhaltung der in Anhang I dargelegten grundlegenden Cybersicherheitsanforderungen nachzuweisen. Hersteller müssen mindestens eines der im CRA festgelegten Konformitätsbewertungsverfahren umsetzen. Dies schließt Änderungen an Produkten, Aktualisierungen harmonisierter Normen und sich weiterentwickelnde Cybersicherheitszertifizierungen ein.

Art und Umfang dieser Bewertung hängen von der Klassifizierung des Produkts ab. Derzeit sind die verfügbaren Informationen zu Produktkategorien noch unvollständig. Gemäß Artikel 7(4) wird erwartet, dass die Europäische Kommission bis zum 11. Dezember 2025 einen Durchführungsrechtsakt erlässt, um die technischen Beschreibungen der in Anhang III festgelegten Klassen I und II wichtiger Produkte sowie der in Anhang IV aufgeführten kritischen Produktkategorie zu definieren. Ein **Entwurf** dieses Rechtsakts befindet sich derzeit in der Entwicklung.

Standard

Wenn das Produkt nicht als wichtig oder kritisch eingestuft ist, kann der Hersteller eine interne Konformitätsbewertung durchführen. Die Mehrheit der betroffenen Produkte fällt unter diese Kategorie. Dies gilt auch für freie und Open-Source-Software, die mit kommerziellen Produkten verbunden ist.

Dienstleistungen, die nicht integraler Bestandteil der Funktionalität eines Produkts sind, sind vom CRA ausgenommen.

Wichtige Produkte, Klasse I

Der Hersteller kann eine interne Bewertung nur dann durchführen, wenn er harmonisierte Normen, gemeinsame Spezifikationen oder europäische Cybersicherheitszertifizierungsschemata anwendet. Beispiele für Produkte der Klasse I sind Passwortmanager, Produkte mit der Funktion eines Virtual Private Network (VPN), Netzwerkmanagementsystem und universelle virtuelle Assistenten für Smart Homes.

Wichtige Produkte, Klasse II

Produkte der Klasse II erfordern immer eine Konformitätsbewertung durch Dritte. Dazu gehören Hypervisoren, manipulationssichere Mikroprozessoren und Mikrocontroller.

Kritisch

Kritische Produkte müssen entweder ein europäisches Cybersicherheitszertifikat gemäß der Verordnung (EU) 2019/881, dem EU-Cybersicherheitsgesetz von 2019, erhalten oder denselben Konformitätsbewertungsverfahren wie Produkte der Klasse II folgen.

Sobald ein Hersteller die Konformitätsbewertung für sein Produkt abgeschlossen hat, muss er anschließend eine Konformitätserklärung in den Sprachen des Mitgliedstaats verfassen, in dem das Produkt verkauft wird. Danach kann er die CE-Kennzeichnung auf seinem Produkt, dessen Verpackung, Begleitdokumentation und Website anbringen.

Zusammenarbeit für Konformität

Der CRA hat die Landschaft der Produktkonformität in der EU grundlegend verändert. Die Navigation durch den CRA und seine komplexen Anforderungen stellt eine der größten Herausforderungen für Hersteller dar, wenn es darum geht, sichere Produkte auf den Markt der Europäischen Union zu bringen, die potenziell mit dem Internet verbunden werden können.

Die Kombination aus den fortschrittlichen sicheren Prozessoren von NXP und den umfassenden Lösungen von Digi bietet Sicherheits-Bausteine, die es Hersteller ermöglichen, die CRA-Anforderungen zu erfüllen.

NXP und Digi — Entwicklung der nächsten Generation von Prozessoren und SOM-Lösungen

Digi International arbeitet mit Herstellern wie NXP Semiconductors zusammen, um Entwickler-Bausteine bereitzustellen, die fortschrittliche Prozessoren und Sicherheitsmethoden nutzen und Hersteller damit bei der Entwicklung von Secure-by-Design Produkten unterstützen, die Anforderungen wie die des CRA und anderer Vorschriften zu erfüllen.

NXPs Sicherheitsstrategie: CRA bereit

Das EdgeLock® Assurance Program von NXP wurde von NXP ins Leben gerufen, um die gereifte Sicherheitsstrategie des Unternehmens zu adressieren. Es dient als Grundlage für Kunden, um Sicherheitsstandards und Vorschriften zu erfüllen, unterstützt den Sicherheitsprozess der Produktentwickler und liefert gleichzeitig Sicherheitsfunktionen für Produkte.

Dieses Programm umfasst die Umsetzung von Best Practices der Branche für sichere Entwicklung sowie eine robuste Unternehmenskultur, die physische und logische Sicherheit adressiert, ebenso wie kontinuierliche Schulungen der Mitarbeiter. Sichere Produktentwicklungsprozesse sind ein integraler Bestandteil des Programms und werden von externen Dritten nach Industriestandards wie ISO 21434, IEC 62443-4-1 und IEC 8001-5-1 zertifiziert.

Produkte von NXP mit Sicherheitsfunktionen werden während des Entwicklungsprozesses von einem Expertenteam des unternehmenseigenen Vulnerability-Analysis-Labors überprüft, um sicherzustellen, dass NXP-Produkte gegen die gängigsten Risikoszenarien gehärtet sind. Darüber hinaus stellt NXP sicher, dass seine Sicherheitsversprechen von unabhängigen Dritten überprüft werden, die strengen Industriestandards wie SESIP (EN 17927) und Common Criteria (ISO 15408) folgen, um sicherzustellen, dass die Komponenten von NXP den höchsten Standards in Bezug auf Sicherheit und Widerstandsfähigkeit entsprechen. Die unabhängigen Dritten überprüfen die Sicherheitsversprechen der NXP-Produkte, die Robustheit solcher Implementierungen gegenüber spezifischen Angriffsarten sowie die Überprüfung gegen öffentlich bekannte Schwachstellen und liefern so modernste Sicherheit für jedes zutreffende Risikoniveau.

Skalierbare Sicherheitsarchitektur und Zuordnung der CRA-Anforderungen

Um die CRA Konformität weiter zu unterstützen, können die Sicherheitsfunktionen der NXP-Produkte den wesentlichen Cybersicherheitsanforderungen des CRA zugeordnet werden, einschließlich Produktkonfiguration, Authentifizierung, Zugriffskontrolle, Datenschutz, Überwachung, Schwachstellenmanagement und Reaktion auf Sicherheitsvorfälle. Die Sicherheitslösungen von NXP sind in unterschiedlichen Sicherheitsstufen verfügbar, von Einsteiger- bis hin zu fortgeschrittenen Funktionen — und ermöglichen Hersteller, den Schutz basierend auf den Risikostufen zu skalieren. Schlüsseltechnologien wie die **EdgeLock Secure Enclave**, **Secure Elements**, und **EdgeLock 2GO** Services bieten robusten Schutz für Zugangsdaten, Sicherheitsmanagement über den gesamten Lebenszyklus und schlüsselfertige Bereitstellung.

NPXs Sicherheitslösungen für CRA konforme Anwendungen

Um ein sicheres und robustes System aufzubauen, müssen wir zunächst den Anker des gesamten Systems auf etwas setzen, dem wir vertrauen. Ein Siliziumchip mit seiner in Hardware verankerten Sicherheitsarchitektur ist schwer anzugreifen, weil er von Natur aus vertrauenswürdig ist. Ein Siliziumchip ist die Grundlage und Basis für alle darauf laufenden Softwarekomponenten. Software — wie Firmware, Kommunikations-Stacks, Betriebssysteme und andere Anwendungen — kann verändert und kompromittiert werden, aber das Silizium ist nicht so leicht zu kompromittieren. Wir nennen das Silizium die “Root of Trust” (RoT) des Systems.

Es gibt keine absolute Sicherheit, da das Spektrum möglicher Angriffe extrem groß ist und zudem die wachsende Komplexität von Anwendungen die Angriffsfläche erheblich vergrößert.

Daher ist es wichtig, mit einem Lösungsanbieter wie Digi zusammenzuarbeiten, der die sicheren Prozessoren von NXP in seine **Digi ConnectCore® system-on-module** integriert und vollständige, Secure-by-Design Lösungen und Bausteine liefert — wie **Digi ConnectCore Cloud Services** und **Digi ConnectCore Security Services** — die Hersteller in die Lage versetzen, sichere Endprodukte zu entwickeln und auszuliefern, ihre Lösungen aus der Ferne zu überwachen und zu verwalten, die Anforderungen des CRA zu erfüllen und sogar zusätzliche Einnahmequellen für das Geschäftsmodell ihres Unternehmens zu..erschließen.

Digis End-to-End Support für CRA Konformität

Europäische und internationale Unternehmen gleichermaßen benötigen praxisnahe, umsetzbare Anleitung zum CRA — und dazu, wie Produkte von Grund auf konform entwickelt werden können.

Digi legt **einen starken Fokus auf Cybersicherheit** und verfolgt den CRA seit seiner ersten Ankündigung. Dabei nutzen wir unsere Erfahrung im Bereich Sicherheit und ordnen unsere Sicherheitsbausteine den Anforderungen dieser wichtigen Verordnung zu. Außerdem verfolgen wir mit unseren Services einen einzigartigen Ansatz, der jeden Aspekt des CRA abdeckt und eine detaillierte Vorgehensweise in klar gegliederten Schritten zur Umsetzung bietet.

“Als wir mit Digi gesprochen haben, war es das erste Mal, dass jemand wirklich darüber gesprochen hat, was wir tun müssen, um den CRA einzuhalten”, berichtet ein Kunde. “Als wir uns mit anderen Anbietern getroffen haben, gaben sie uns nur allgemeine Übersichten über das Gesetz.”

Die Embedded Lösungen und Services von Digi sind bewusst so konzipiert, dass sie Kunden bei der Einhaltung der CRA-Anforderungen und -Verpflichtungen unterstützen. Digi arbeitet mit jedem Kunden zusammen, um ein Servicepaket zu erstellen, das auf seine spezifischen Bedürfnisse zugeschnitten ist.

Digis Konformität orientiertes Ökosystem

Digi bietet eine **Komplettlösung mit** von Cloud-to-Connectivity-Services an, einschließlich **Digi ConnectCore system-on-modules** (SOMs), Software und Tools, sowie **Digi ConnectCore Security Services** und **Digi ConnectCore Cloud Services**, die ein integriertes Ökosystem mit eingebauter Sicherheit bilden. Unsere Lösungen unterstützen die Entwicklung konformer, Secure-by-Design Digitalprodukte mit proaktivem Schwachstellenmanagement, sicheren Software-Updates sowie Remote-Konfiguration, -Überwachung und -Wartung.

Mit dem vollständigen Ökosystem von Digi können Hersteller während des gesamten Produktlebenszyklus zuverlässig die CRA Konformität aufrechterhalten und gleichzeitig sowohl die Komplexität als auch die Markteinführungszeit reduzieren. Unser integrierter Ansatz hilft nicht nur dabei, aktuelle Anforderungen zu erfüllen, sondern versetzt Organisationen auch in die Lage, sich nahtlos an zukünftige regulatorische Änderungen anzupassen.

Neben unserem speziell entwickelten Portfolio und unseren Services bietet Digi auch verschiedene Schulungsressourcen an, darunter ein einstündiges Webinar, das sich damit befasst, **wie Ingenieure die Herausforderungen des CRA bewältigen können**.

Digi TrustFence

Entwickelt für unternehmenskritische Anwendungen, hilft **Digi TrustFence®** Entwicklern dabei, dynamische, adaptive Sicherheit direkt in IoT-Produkte zu integrieren. Dies unterstützt sowohl die „Security-by-Design“ als auch „Security-by-Default“ Grundsätze des CRA durch Funktionen wie sichere Konfiguration, Secure Boot, sichere Konsole, sichere Konsole, sichere Software-Updates, verschlüsseltes Dateisystem sowie geschützte Hardware und Schnittstellen.

Digi ConnectCore Security Services

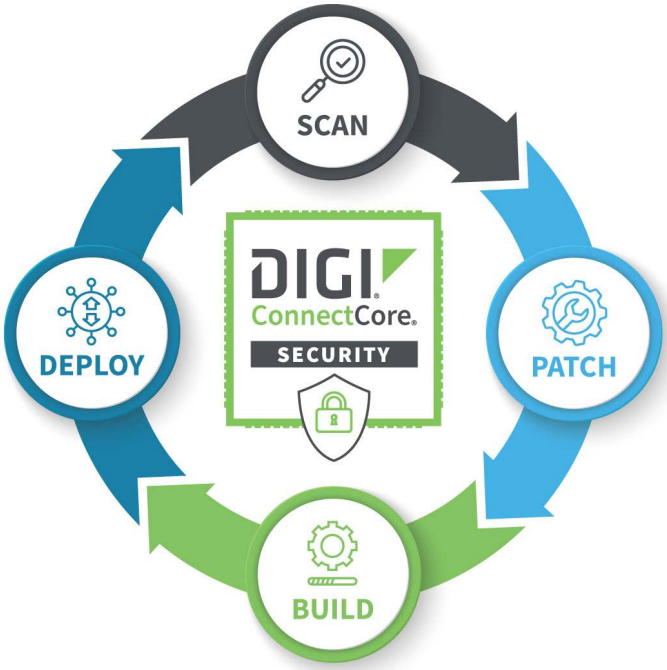
Digi ConnectCore Security Services bieten eine Reihe von Tools, um Unternehmen bei der Erfüllung der CRA-Anforderungen für Schwachstellenmanagement und -meldung zu unterstützen, einschließlich der 24-Stunden-Meldepflicht für aktiv ausgenutzte Schwachstellen und schwerwiegende Vorfälle.

Dies umfasst die kontinuierliche Analyse und Überwachung einer kundenspezifischen SBOM, die auf Digi ConnectCore SOMs läuft, auf Sicherheitslücken. Um kritische Probleme zu beheben, bieten die Services einen kuratierten Schwachstellenbericht, eine Sicherheitsschicht für Software mit Patches und Korrekturen für häufige Schwachstellen sowie Expertenberatung und Supportleistungen.

Digi ConnectCore Cloud Services

Digi ConnectCore Cloud Services basieren auf der **Digi Remote Manager®** (Digi RM) Plattform und helfen Herstellern, ihre Geräte aktuell zu halten und bieten umfangreiche Funktionen für Prozessautomatisierung, Überwachung und Remote-Gerätemanagement.

Durch die Kombination bewährter Standardhardware mit dem führenden Fachwissen und der Erfahrung von Digi ermöglichen ConnectCore Cloud Services Hersteller die Entwicklung konformer, vernetzter Geräte, die Kunden durch automatisierte Massen-Updates von Firmware und Software, bidirektionale Kommunikation, Echtzeit-Benachrichtigungen und detaillierte Berichte über Gerätezustände und Netzwerkgesundheit eine überlegene Qualität und Benutzerfreundlichkeit bieten.



Digi Wireless Design Services

Wenn Sie mit Embedded-Lösungen von Digi arbeiten und technische Unterstützung benötigen, kann Ihnen unser **Wireless Design Services** (WDS) Team helfen. WDS kann Ihr Entwicklungsteam in jeder Phase unterstützen, sei es bei Produktdesign und -entwicklung, Zertifizierungen, Softwareentwicklung, schneller Markteinführung oder fortlaufender Zusammenarbeit, um dauerhafte Produktkonformität sicherzustellen.

Digi Embedded Yocto (DEY)

Eine Open-Source-Linux Distribution basierend auf dem Yocto Project™, **Digi Embedded Yocto** (DEY) ist speziell für unsere SOMs entwickelt. Sie hilft Embedded-Entwicklern, ihre CRA Konformität Verpflichtungen zu erfüllen, durch eine Kombination aus von Digi verwalteter Softwarepflege, robuster **Patch-Policy** und vollständiger Integration mit Digi TrustFence sowie Digi ConnectCore Security und Cloud-Services zu erfüllen.

Digi bietet umfassende CRA-Konformität Unterstützung, einschließlich automatisierter Schwachstellenanalys, sicherer Remote-Updates und Expertenberatung während des gesamten Produktlebenszyklus.

Konformität mit dem CRA: Nutzung der Digi Security Bausteine

Im Folgenden erläutern wir, wie die Digi ConnectCore Lösung Ihnen hilft, die Anforderungen des CRA zu erfüllen.

Teil I: Produktbezogene Cybersicherheitsanforderungen

In den Tabellen auf den folgenden Seiten haben wir die vierzehn Cybersicherheitsanforderungen in Bezug auf Produkteigenschaften gemäß Anhang I, Teil I aufgeführt. Wir haben die Anforderungen umfassend angewendet und diese Digi TrustFence, Digi ConnectCore Security Services, Digi ConnectCore Cloud Services und natürlich unserem DEY-Betriebssystem zugeordnet. Werfen wir einen genaueren Blick auf ein paar dieser Anforderungen.

- **Anhang I, Teil I 2(a)** Produkte werden ohne bekannte ausnutzbare Schwachstellen ausgeliefert. Digi ConnectCore Security Services ermöglichen benutzerdefinierte Scans der Software Bill of Materials (SBOM), um häufige Schwachstellen und Gefährdungen (CVEs) zu prüfen, Fehlalarme zu entfernen und Hersteller zu ermöglichen, sich auf die kritischsten Probleme zu konzentrieren. Zusätzlich können Hersteller von unserer Meta Digi Security Schicht profitieren, die eine Sammlung vorintegrierter Sicherheitspatches für DEY, Board Support Package (BSP), Linux Kernel und Bootloader enthält.
- **Anhang I, Teil I 2(c)** Schwachstellen können durch die sichere Software-Update-Funktion behoben werden, die in Digi TrustFence und unseren Digi ConnectCoure Cloud Services enthalten ist, um solche Patches und Korrekturen sicher und zuverlässig remote „over-the-air“ (OTA) bereitzustellen.

Diese Bewertung zeigt unsere Software, Werkzeuge, Funktionen und Prozesse, die Kunden helfen, das Gesetz einzuhalten, schneller auf den Markt zu kommen und die Konformität während des gesamten Produktlebenszyklus zu sichern.

Es gibt einige Anforderungen, die nicht auf die Digi Sicherheitsbausteine zutreffen, aber für ein auf ConnectCore basierendes Endprodukt gelten könnten. Beispielsweise muss ein HERSTELLER, der eine Anwendung mit einem Digi ConnectCore SOM entwickelt, die CRA-Anforderungen im Endprodukt erfüllen. Hersteller können potenziell anfällige Hardware und Software in ihren Endprodukten einsetzen, weshalb sie sorgfältig abschätzen müssen, welche Maßnahmen im Verlauf der CRA-Umsetzung ergriffen werden müssen.

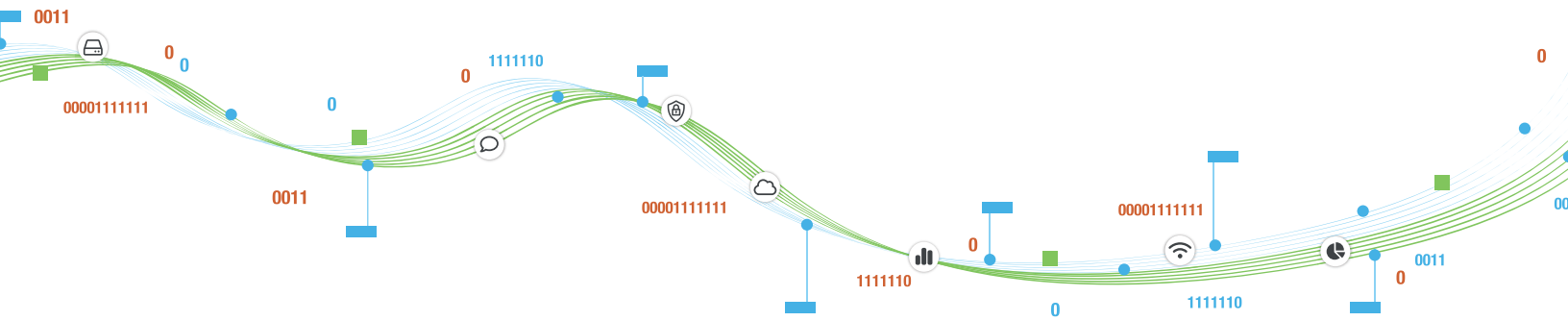
Teil II: Anforderungen zum Umgang mit Schwachstellen

Die letzte Tabelle umfasst die acht Anforderungen zum Umgang mit Schwachstellen aus Anhang I, Teil II. Nach dem gleichen Ansatz wie in Teil I haben wir jede dieser Anforderungen sorgfältig unseren Sicherheitsbausteinen zugeordnet. Werfen wir einen genaueren Blick auf einige dieser Anforderungen.

- **Anhang I, Teil II 1** Unsere bewährte Lösung, zusammen mit DEY und Digi ConnectCore Security Services, erleichtert es Herstellern, Schwachstellen und in Produkten enthaltene Komponenten zu identifizieren und zu dokumentieren, indem eine individuelle SBOM erstellt wird, die zumindest die Top-Level-Abhängigkeiten abdeckt.
- **Anhang I, Teil II 7** Digi TrustFence und Digi ConnectCore Cloud Services bieten zudem Mechanismen, um Produktupdates sicher zu verteilen und so sicherzustellen, dass Schwachstellen zeitnah behoben oder gemindert werden und, falls zutreffend, Sicherheitsupdates automatisiert erfolgen. Unsere Cloud-Services gewährleisten sichere Edge-to-Cloud-Kommunikation durch Unterstützung von TLS (Transport Layer Security), zertifikatsbasierter Authentifizierung und Verschlüsselung. Darüber hinaus können mit der Template-Funktion komplette Geräteflotten im Feld automatisch gescannt, aktualisiert und gemäß der festgelegten Konfiguration gewartet werden. Durch die Nutzung von Templates können unsere Kunden Zeit sparen, Fehler reduzieren, den Aufwand minimieren und die Verwaltung im großen Maßstab erleichtern, wenn Konfigurationsupdates erforderlich sind, sowie Konsistenz und Standardisierung über alle im Feld eingesetzten Geräte hinweg sicherstellen.

Der Umfang dieser Analyse konzentriert sich auf Digi ConnectCore. Hersteller, die Produkte auf Basis unserer SOMs entwickeln, können von unseren Mehrwertlösungen profitieren, müssen jedoch bestimmte Anstrengungen unternehmen, um die CRA-Verpflichtungen und -Anforderungen sowie deren Meilensteine einzuhalten, um ein Produkt auf den Markt zu bringen oder bestehende Produkte weiter zu verkaufen.

Selbstverständlich können wir einen Termin mit Ihrem Vertriebsmitarbeiter vereinbaren, um eine detaillierte Analyse dieser Anforderungen und die Umsetzung der Digi-Sicherheitsbausteine für ein spezifisches Projekt durchzuführen.

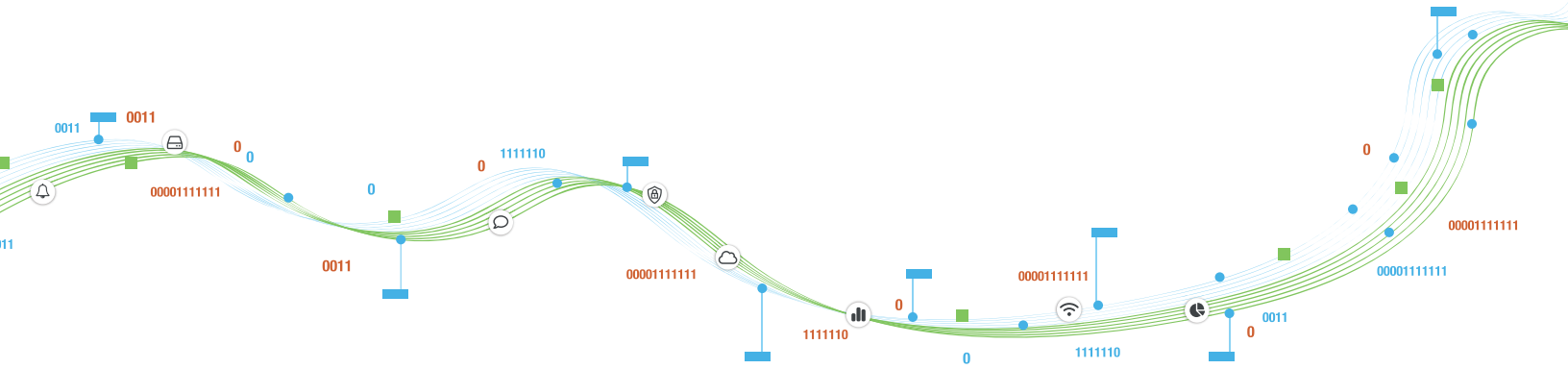


Konformität mit dem CRA: Nutzung der Digi Security Bausteine (I)

Teil I	Beschreibung	Digi TrustFence	Digi ConnectCore Security Services	Digi ConnectCore Cloud Services	Digi Embedded Yocto
(1)	Produkte müssen so entworfen, entwickelt und hergestellt werden, dass ein angemessenes Maß an Cybersicherheit auf der Grundlage der Risiken gewährleistet ist	TrustFence gesamt	Security services komplett	Cloud services gesamt	DEY komplett
(2) (a)	Produkte müssen ohne bekannte ausnutzbare Schwachstellen bereitgestellt werden	N/A	Benutzerdefinierte SBOM Scans, meta-digi-security	Digi RM Vulnerability Patch Policy	Digi owned software maintenance
(2) (b)	Produkte müssen mit einer standardmäßig sicheren Konfiguration bereitgestellt werden	TrustFence komplett	N/A	N/A	Hardened DEY
(2) (c)	Produkte müssen sicherstellen, dass Schwachstellen durch Sicherheitsupdates behoben werden können	Sichere Software Updates	meta-digi-security, Beratung und Support	Sichere remote OTA Software Updates	Sicheres Software Updates, dual boot Konfiguration
(2) (d)	Produkte müssen sicherstellen, dass sie vor unbefugtem Zugriff geschützt sind	Sichere Konsole, sicheres JTAG	N/A	N/A	SSH/TLS
(2) (e)	Produkte müssen die Vertraulichkeit von gespeicherten, übertragenen oder anderweitig verarbeiteten Daten, personenbezogen oder andere, schützen	Verschlüsseltes Dateisystem Dateien (hardwaregebunden) Datei(hardwaregebunden)	N/A	Dateisystemzugriff, TLS, zertifikatsbasierte Authentifizierung und Verschlüsselung	Verschlüsselung, WPA3, FIPS 140-2/3 (zusätzliche Kosten)
(2) (f)	Produkte müssen die Integrität von gespeicherten, übertragenen oder anderweitig verarbeiteten Daten, personenbezogen oder andere, Befehlen, Programmen und Konfigurationen schützen	Secure boot / authentifiziertes Dateisystem	N/A	Dateisystemzugriff, TLS, zertifikatsbasierte Authentifizierung und Verschlüsselung	TLS, read-only Dateisystem
(2) (g)	Produkte dürfen nur Daten, personenbezogen oder andere, verarbeiten, die angemessen, relevant und auf das notwendige Maß beschränkt sind	N/A	N/A	Benutzerdefinierte Daten Streams	N/A
(2) (h)	Produkte müssen die Verfügbarkeit wesentlicher und grundlegender Funktionen gegen Denial-of-Service-Angriffe schützen	N/A	N/A	N/A	Best Practices für Sicherheit eingebetteter Systeme
(2) (i)	Produkte müssen die negativen Auswirkungen der Produkte selbst oder verbundener Geräte auf die Verfügbarkeit von Diensten anderer Geräte oder Netzwerke minimieren	N/A	N/A	N/A	Best Practices für Sicherheit eingebetteter Systeme
(2) (j)	Produkte müssen so entworfen, entwickelt und hergestellt werden, dass Angriffsflächen, einschließlich externer Schnittstellen, begrenzt werden	Secure Boot, sichere Konsole, sicheres JTAG, Manipulationserkennung	meta-digi-security, Beratung und Support	N/A	N/A
(2) (k)	Produkte müssen so entworfen, entwickelt und hergestellt werden, dass die Auswirkungen eines Vorfalls durch geeignete Ausnutzungsvermeidungsmechanismen und -techniken reduziert werden	Manipulationserkennung	N/A	Templates	N/A
(2) (l)	Produkte müssen sicherheitsrelevante Informationen bereitstellen, indem relevante interne Aktivitäten aufgezeichnet und überwacht werden	Manipulationserkennung	N/A	Security monitoring agent	N/A
(2) (m)	Produkte müssen den Nutzern die Möglichkeit bieten, dauerhaft alle Daten und Einstellungen sicher und einfach zu entfernen und, wenn solche Daten auf andere Produkte oder System übertragen werden können, sicherstellen, dass dies auf sichere Weise geschieht	N/A	N/A	Dateizugriff, Digi RM Daten-/Konfigura-tions-Management	N/A

Konformität mit dem CRA: Nutzung der Digi Security Bausteine (II)

Teil II	Beschreibung	Digi TrustFence	Digi ConnectCore Security Services	Digi ConnectCore Cloud Services	Digi Embedded Yocto
(1)	Hersteller müssen ein Softwarestückverzeichnis in einem gängigen und maschinenlesbaren Format erstellen	N/A	BenutzerdefinierteSBOM Erstellung	N/A	DEY SBOM
(2)	Hersteller müssen Schwachstellen unverzüglich beheben	N/A	meta-digi-security, Beratung und Support	Sichere remote OTA Software Updates, Vorlagen	DEY regular releases
(3)	Hersteller müssen wirksame und regelmäßige Tests und Überprüfungen der Produktsicherheit durchführen	N/A	Benutzerdefinierte SBOM scans	Digi RM Vulnerability Patch Policy	DEY Patch Policy
(4)	Hersteller müssen Informationen über behobene Schwachstellen weitergeben und öffentlich bekannt machen	N/A	Security Services komplett	Digi Security Center	Digi Security Center
(5)	Hersteller müssen eine Richtlinie für koordinierte Schwachstellenmeldungen einführen und durchsetzen	N/A	N/A	Digi RM Vulnerability Patch Policy, Digi Security Center	DEY Patch Policy, Digi Embedded GitHub, Digi Security Center
(6)	Hersteller müssen den Austausch von Informationen über potenzielle Schwachstellen erleichtern, unter anderem durch Bereitstellung einer Kontaktadresse für die Meldung entdeckter Schwachstellen	N/A	N/A	Digi security form	Digi security form
(7)	Hersteller müssen Mechanismen bereitstellen, um Updates sicher zu verteilen, damit Schwachstellen rechtzeitig behoben oder gemindert werden	Sichere Software Updates	N/A	Sichere remote OTA Software Updates, Templates, TLS, zertifikatsbasierte Authentifizierung und Verschlüsselung	N/A
(8)	Hersteller müssen sicherstellen, dass Sicherheitsupdates, sobald verfügbar, unverzüglich und kostenlos verteilt werden, begleitet von Hinweismeldungen, die den Benutzern relevante Informationen einschließlich potenzieller Maßnahmen bereitstellen	N/A	N/A	Sichere remote OTA Software Updates, Templates	DEY Patch Policy, Digi Embedded GitHub



Das Digi Ökosystem: Integrierte CRA-Konformität

Eine der größten Stärken des Digi-Portfolios ist der integrierte Ansatz zur CRA-Konformität. Digi-Lösungen sind Secure-by-Design und werden unterstützt von Digi TrustFence, Digi ConnectCore Security Services, Digi ConnectCore Cloud Services und Digi Embedded Yocto (DEY). Diese bilden eine integrierte Hardware- und Softwarelösung mit von Grund auf eingebauter Sicherheit.

Das Digi-Ökosystem bietet eine umfassende Abdeckung für wichtige CRA-Anforderungen:

- ✓ **SBOM management:** Tools zur Erstellung und Pflege eines Softwarestückverzeichnisses
- ✓ **Umgang mit Schwachstellen:** Häufiges Scannen nach Schwachstellen, die nach der ursprünglichen Produkteinführung auftreten
- ✓ **Reporting tools:** Enthält kuratierte Schwachstellenberichte, die kritische Probleme hervorheben
- ✓ **Behebung von Schwachstellen:** Sicherheitsschicht für Software, die Patches und Korrekturen für häufige Schwachstellen umfasst
- ✓ **Sicherheitswartung:** Sichere und zuverlässige Remote-OTA-Softwareupdates
- ✓ **Geräteflottenmanagement:** Ermöglicht Prozessautomatisierung, Überwachung, Remote-Gerätemanagement und Kostenreduktion
- ✓ **Experten-Support:** Beratungs- und Unterstützungsleistungen für die Integration von Patches und Korrekturen

Mit dem vollständigen Ökosystem von Digi aus SOMs, Software, Tools und Services können Hersteller ihre Konformität mit dieser Gesetzgebung zuverlässig beschleunigen, die Markteinführungszeit verkürzen und was noch wichtiger ist, die Konformität während des gesamten Produktlebenszyklus aufrechterhalten. Dieser integrierte Ansatz erfüllt nicht nur die aktuellen CRA-Anforderungen, sondern positioniert Organisationen auch so, dass sie sich nahtlos an zukünftige regulatorische Änderungen anpassen können.

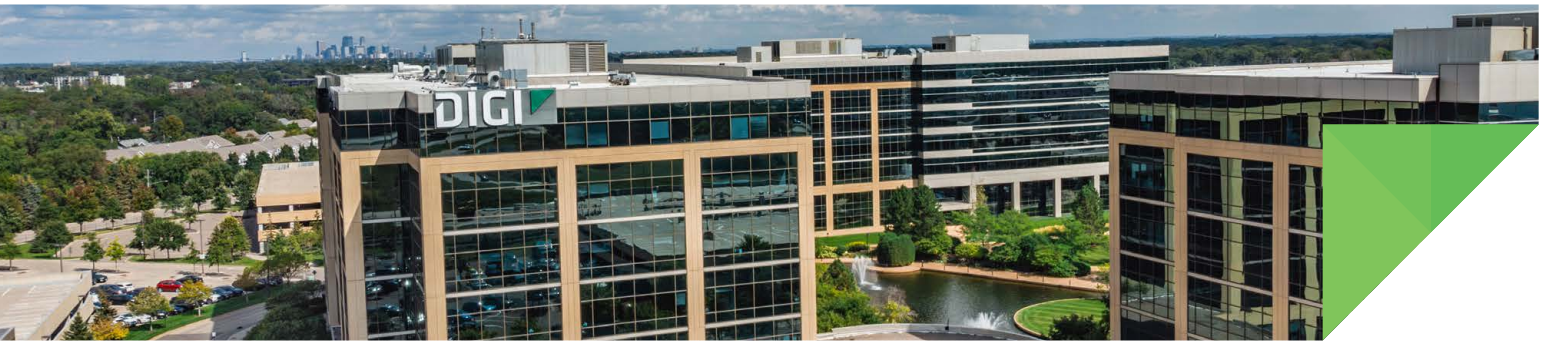
Fazit

Der CRA stellt einen grundlegenden Wandel in der Landschaft digitaler Produkte dar. Er etabliert Cybersicherheit als grundlegendes, nicht verhandelbares Element des Produktlebenszyklus.

Während der CRA seinen Ursprung in Europa hat, erstreckt sich sein Einfluss bereits weltweit. Durch die frühzeitige Umsetzung seiner Grundsätze können sich Organisationen auf neue Vorschriften in anderen Regionen vorbereiten und die Einhaltung von Vorschriften von einer Herausforderung in eine Chance für nachhaltiges Wachstum und langfristige Marktführerschaft verwandeln.

Organisationen, die die CRA-Konformität strategisch angehen, werden auch über die reine Einhaltung von Vorschriften hinausgehende Chancen entdecken. Durch die Integration von Sicherheit über den gesamten Produktlebenszyklus hinweg—von der Konzeption über die Entwicklung, Produktion, Implementierung und Wartung —können Hersteller ein tieferes Kundenvertrauen aufbauen, kostspielige Sicherheitsvorfälle reduzieren und widerstandsfähigere Produkte schaffen, die den Test der Zeit bestehen.

Fordern Sie eine kostenlose einstündige Digi-Sicherheitsberatung an



Warum Digi?

Digi ist ein umfassender IoT-Lösungsanbieter, der jeden Aspekt Ihres Projekts unterstützt, von unternehmenskritischer Kommunikationstechnik bis hin zu Design- und Bereitstellungsdiensten, um Ihre Anwendung sicher, zuverlässig und mit höchster Leistung zu entwerfen, zu installieren, zu testen und in Betrieb zu nehmen.

Digi entwickelt seine Produkte für hohe Zuverlässigkeit, hohe Leistung, Sicherheit, Skalierbarkeit und Vielseitigkeit, sodass Kunden eine lange Lebensdauer erwarten können, sich schnell an sich ändernde Systemanforderungen anpassen und zukünftige Technologien übernehmen können, sobald diese verfügbar sind. Digi Embedded-Module, Router, Gateways und Infrastrukturmanagement-Lösungen unterstützen die neuesten vernetzten Anwendungen in verschiedenen Branchen, von Unternehmen über Transport, Energie, Industrie bis hin zu Smart-City-Anwendungen.

Unsere Lösungen ermöglichen die Konnektivität von standardbasierten und proprietären Geräten, Vorrichtungen und Sensoren und gewährleisten zuverlässige Kommunikation über nahezu jede Form von drahtlosen oder kabelgebundenen Systemen. Unsere integrierte Plattform für Remote-Management hilft, die Bereitstellung zu.

Unternehmenshintergrund

- Digi verbindet das „Internet of Things“ — Geräte, Fahrzeuge, Ausrüstung und Assets — seit 1985
- Digi ist an der NASDAQ-Börse notiert: DGII
- Mit Hauptsitz in den Twin Cities in Minnesota beschäftigt Digi weltweit über 800 Mitarbeiter und hat weltweit über 100 Millionen Geräte vernetzt

Als IoT-Lösungsanbieter setzt Digi bewährte Technologie für unsere Kunden ein, damit sie Netzwerke aktivieren und neue Produkte auf den Markt bringen können. Maschinenkonnektivität, die unermüdlich zuverlässig, sicher, skalierbar und verwaltet ist — und immer dann funktioniert, wenn man sie am dringendsten braucht. Das ist Digi.

Nächste Schritte

- Bereit mit einem Digi-Experten zu sprechen? **Kontaktieren Sie uns**
- Möchten Sie mehr von Digi hören? **Newsletter abonnieren**
- Jetzt Digi-Lösungen kaufen: **Kaufanleitung**

Kontaktieren Sie einen Digi Experten und legen Sie noch heute los.

PH: 877-912-3444
www.digi.com

Digi International Worldwide Headquarters
9350 Excelsior Blvd. Suite 700
Hopkins, MN 55343

/digi.international @DigiDotCom /digi-international