CRA EVIDENCE WHITEPAPER

Die EU-Cyberresilienz-Verordnung: ein praktischer Compliance-Leitfaden

Whitepaper für Hersteller, Einführer und Händler von Produkten mit digitalen Elementen.

Version	1.0
Status	Lebendes Dokument
Grundlage	Regulation (EU) 2024/2847

Änderungsverlauf

Die nachstehende Tabelle dokumentiert die wesentlichen Änderungen dieses Leitfadens. Spätere Aktualisierungen werden hier mit Datum und Kurzbeschreibung ergänzt.

Version	Datum	Beschreibung
1.0	17. Mai 2026	Erste öffentliche Veröffentlichung. Strukturparität zur englischen Fassung Welle 2 bis 8: Klassifizierung nach Kernfunktionalität, Cloud-Anteile am Produkt, Lieferketten-Pflichten, neuer Abschnitt zur wesentlichen Änderung, Festlegung des Supportzeitraums, Komponenten-Due-Diligence, Meldefristen nach Artikel 14, Korrekturmaßnahmen sowie Neuordnung des Schwachstellenmanagement-Kapitels.

Inhalt

Zusammenfassung

IN 60 SEKUNDEN

Worum es geht: vernetzte Hardware- und Softwareprodukte, die auf dem EU-Markt bereitgestellt werden. Cybersicherheit wird als Produkt-Compliance-Anforderung behandelt, nicht als Best Practice.

Ab wann es greift: Meldepflichten nach Artikel 14 ab dem 11. September 2026; vollständige technische Pflichten, Dokumentationspflichten und CE-Kennzeichnung ab dem 11. Dezember 2027.

Was Sie erstellen müssen: Cybersicherheits-Risikobewertung, SBOM, technische Dokumentation, Benutzerinformationen und Anleitungen, EU-Konformitätserklärung, CE-Kennzeichnung sowie Meldungen zu Sicherheitsvorfällen und Schwachstellen nach Artikel 14.

Wer handeln muss

Hersteller tragen die Hauptlast. Einführer und Händler haben Sorgfaltsprüfungen, bevor sie Produkte bereitstellen.

Was sich ändert

Cybersicherheit wird Teil der Produkt-Compliance: sichere Entwicklung, Schwachstellenmanagement, Dokumentation, CE-Kennzeichnung und Maßnahmen nach dem Inverkehrbringen.

Erste Frist

Die Meldung nach Artikel 14 beginnt am **11. September 2026** für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle.

Vollständige Anwendung

Die vollständige technische Compliance gilt ab dem **11. Dezember 2027**. Frühere Produkte sind nach einer wesentlichen Änderung erfasst, die Meldepflicht gilt jedoch weiterhin.

Nachweisrückgrat

Die technische Dokumentation braucht Risikobewertung, SBOM, Begründung des Supportzeitraums, Testnachweise, Benutzerinformationen, Erklärung und Nachweise für die grundlegenden Cybersicherheitsanforderungen.

Konformitätsweg

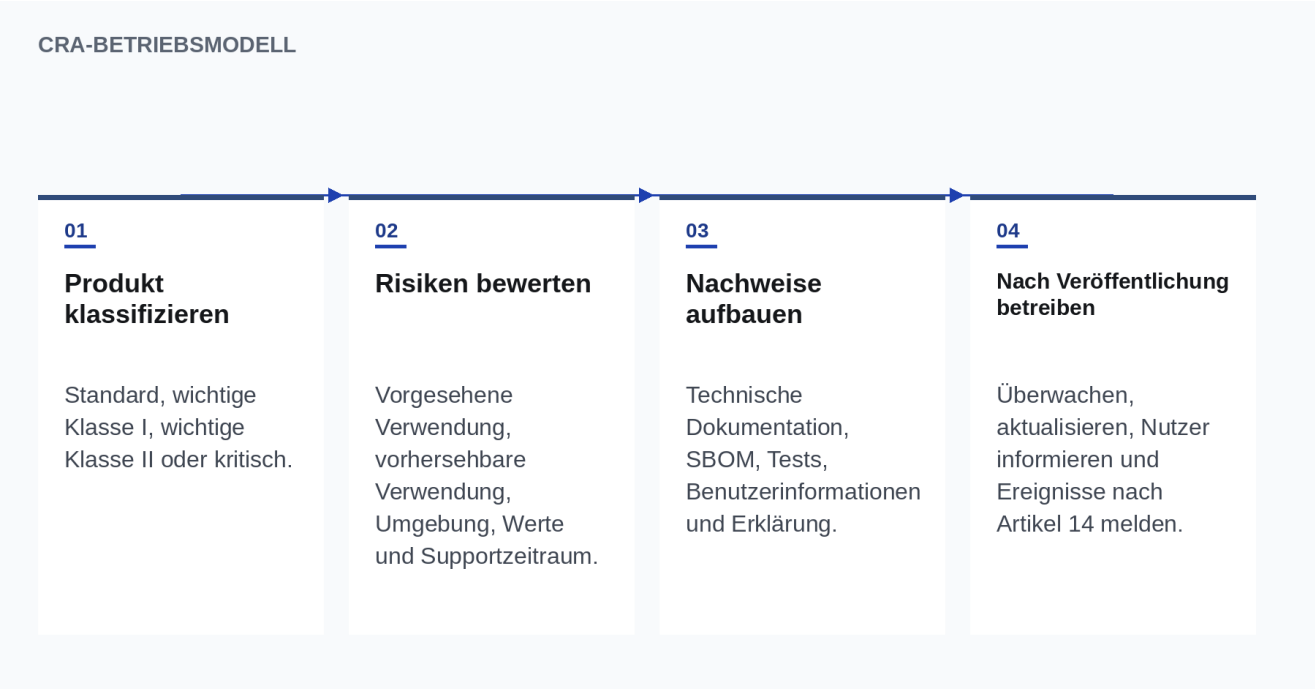
Die meisten Produkte können Modul A nutzen. Wichtige und kritische Produkte benötigen möglicherweise eine notifizierte Stelle oder einen EU-Cybersicherheitszertifizierungsweg.

Was ist die Cyberresilienz-Verordnung?

Regulation (EU) 2024/2847, der Cyber Resilience Act (CRA), formal die Cyberresilienz-Verordnung, ist der erste EU-weite Rahmen, der Cybersicherheit zu einer verbindlichen Anforderung für Produkte mit digitalen Elementen auf dem EU-Markt macht. Der verbindliche Text ist auf EUR-Lex verfügbar.

Der CRA gilt für Hersteller, Einführer und Händler von vernetzter Hardware und Software. Er erfasst Produkte von Verbraucher-IoT-Geräten bis zu industriellen Steuerungssystemen. Die praktische Änderung ist klar: Cybersicherheit muss als Teil der Produkt-Compliance gestaltet, nachgewiesen, gepflegt und überwacht werden.

Verstöße gegen die grundlegenden Cybersicherheitsanforderungen oder die Pflichten der Artikel 13 und 14 können zu Bußgeldern von bis zu 15 Millionen EUR oder 2,5 % des weltweiten Jahresumsatzes führen, je nachdem, welcher Betrag höher ist. Es gibt niedrigere Stufen: bis zu 10 Millionen EUR oder 2 % bei Verstößen gegen andere genannte Pflichten und bis zu 5 Millionen EUR oder 1 % bei der Übermittlung unrichtiger, unvollständiger oder irreführender Informationen an notifizierte Stellen oder Marktüberwachungsbehörden. Marktüberwachungsbehörden können außerdem Korrekturmaßnahmen verlangen, die Bereitstellung beschränken, Produkte vom Markt nehmen oder Rückrufe anordnen.



Wichtige Termine für die Compliance-Planung

Der CRA trat am **10. Dezember 2024** in Kraft. Die praktische Compliance-Arbeit verteilt sich auf drei Meilensteine: notifizierte Stellen im **Juni 2026**, Meldungen im **September 2026** und vollständige technische Compliance im **Dezember 2027**.

HINWEIS

Aktueller Stand der Kommissionsleitlinien: Die Europäische Kommission hat am 3. März 2026 den Entwurf von CRA-Leitlinien veröffentlicht. Die Konsultation endete am 13. April 2026. Die Leitlinien sind nicht endgültig, aber sie sind als Planungsmaterial nützlich: Inverkehrbringen, freie und Open-Source-Software, Supportzeiträume, wesentliche Änderungen, Produktklassifizierung, Komponenten-Due-Diligence, entfernte Datenverarbeitung, Schwachstellenbehandlung und Überschneidungen mit anderem EU-Recht. Grenzfragen zum AI Act und zu DORA können weitere Klarstellung erfordern.

10. Dezember 2024

Inkrafttreten

Übergangsfrist beginnt

11. Juni 2026

Notifizierte Stellen

Kapitel IV gilt

11. September 2026

Meldung

Meldepflicht nach Artikel 14 beginnt

11. Dezember 2027

Vollständige Anwendung

Technische Anforderungen, CE-Kennzeichnung, Dokumentation und Konformitätsbewertung

ZUERST ERLEDIGEN

Beginnen Sie mit der Meldebereitschaft. Die Frist nach Artikel 14 kommt vor der vollständigen technischen Compliance und gilt für Produkte, die bereits auf dem EU-Markt sind.

Da die Meldepflicht am **11. September 2026** beginnt, sollte Meldebereitschaft der erste Umsetzungsstrang sein: **Erkennung, Triage, Nutzerbenachrichtigung und Behördenmeldungen** müssen funktionieren, bevor die vollständige technische Compliance fällig wird.

Produkte mit digitalen Elementen, die vor dem 11. Dezember 2027 in Verkehr gebracht wurden, unterliegen den technischen Anforderungen des CRA nur dann, wenn sie ab diesem Datum wesentlich verändert werden. Die Meldepflicht nach Artikel 14 ist anders. Sie gilt für alle Produkte im Anwendungsbereich, auch für Produkte, die vor dem 11. Dezember 2027 in Verkehr gebracht wurden.

Der CRA über den Produktlebenszyklus

SCHRITT 01

Produktumfang festlegen

Scope, Klassifizierung, Supportzeitraum und Risikoanalyse

SCHRITT 02

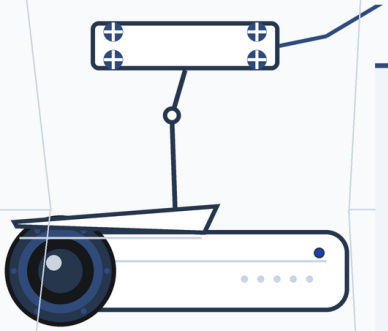
Sicher entwickeln

Sichere Defaults, Codeanalyse, SBOM und Deps-Kontrolle

SCHRITT 03

Validieren und dokumentieren

Tests, Vuln-Triage, technische Doku und Nutzerinfos



SCHRITT 04

In Verkehr bringen

EU-DoC, CE-Kennzeichnung und Freigabe

SCHRITT 05

Überwachen

CVEs, Hinweise, Exploit-Aktivität, Sicherheitsupdates und Offenlegung

SCHRITT 06

Kooperieren

Meldungen nach Artikel 14, Nutzerhinweise, Behördenanfragen und Supportende

Vernetzte IP-Kamera vom Produktplan bis zur Nachmarktunterstützung nach dem CRA

Welche Produkte in den Anwendungsbereich fallen

Anwendungsbereich und Ausnahmen

Der CRA gilt für Hardware- und Softwareprodukte, deren vorgesehene oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte Datenverbindung zu einem Gerät oder Netz einschließt. Dazu gehören Computer, Smartphones, Netzwerktechnik, IoT-Geräte, industrielle Steuerungssysteme und datenverarbeitende Anwendungen.

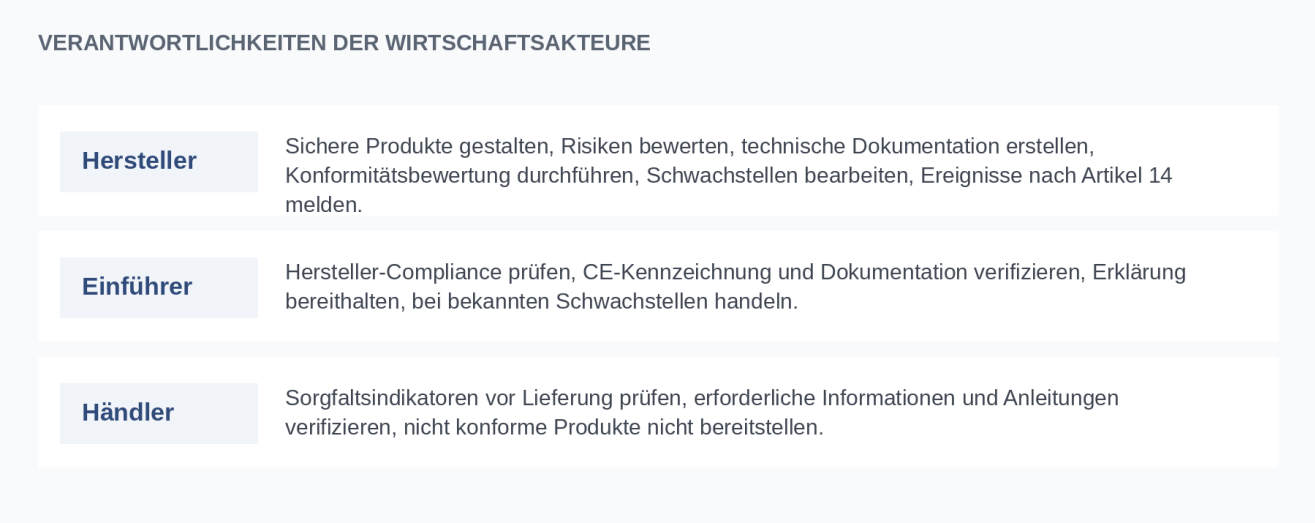
Die folgenden Kategorien sind ausdrücklich ausgenommen:

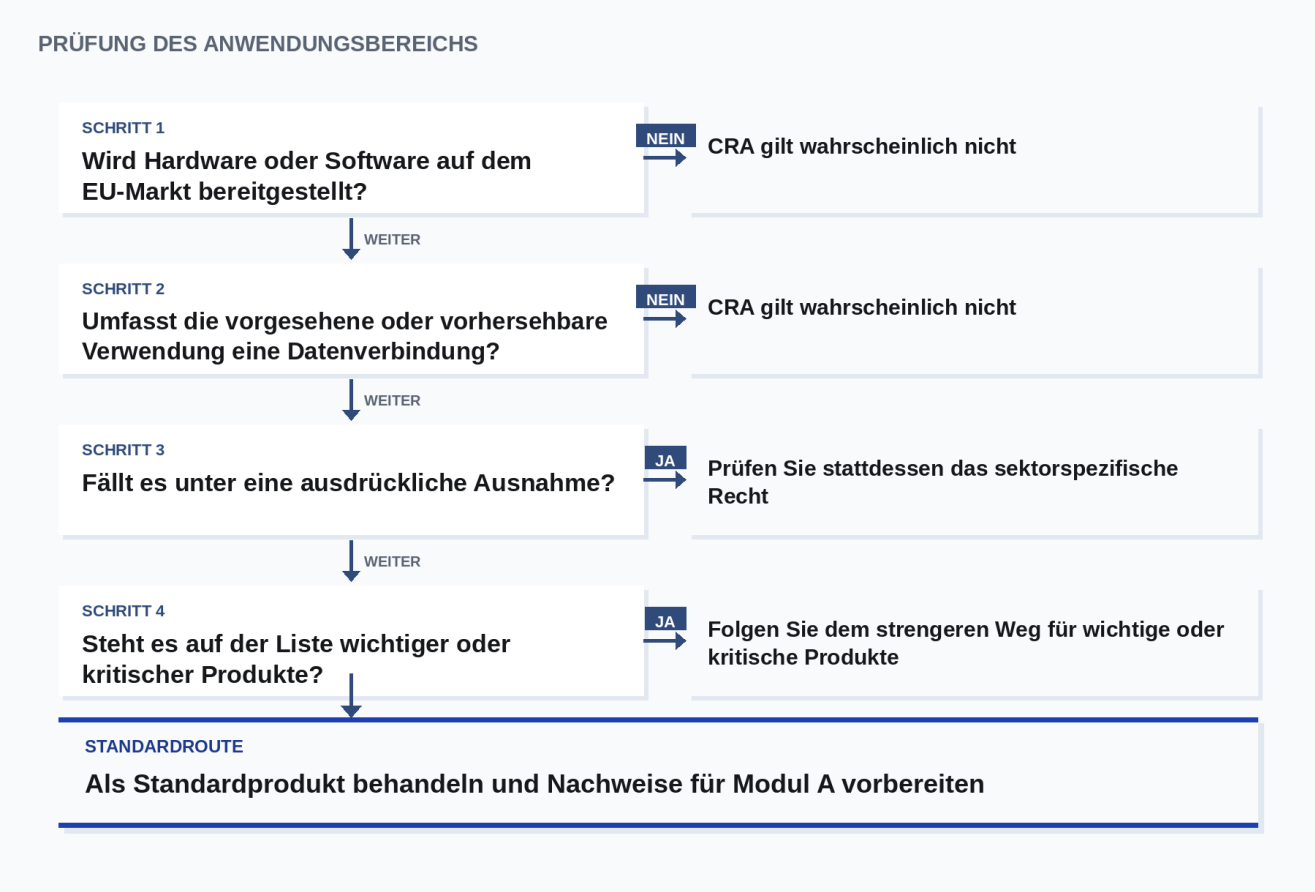
- Medizinprodukte und In-vitro-Diagnostika, die unter Verordnung (EU) 2017/745 und 2017/746 fallen
- Kraftfahrzeugsysteme, die unter Verordnung (EU) 2019/2144 fallen
- Luftfahrtausrüstung, die unter Verordnung (EU) 2018/1139 fällt
- Schiffsausrüstung, die unter Richtlinie 2014/90/EU fällt
- Produkte, die ausschließlich für Zwecke der nationalen Sicherheit oder Verteidigung entwickelt wurden
- Rein mechanische Produkte ohne digitale Elemente oder Netzwerkanbindung

Wenn keine klare Ausnahme greift, gehen Sie davon aus, dass Ihr vernetztes Produkt in den Anwendungsbereich fällt.

HINWEIS

Maßgeschneiderte Produkte: eine enge Ausnahme. Wenn Sie ein Produkt für einen bestimmten gewerblichen Nutzer auf Grundlage einer schriftlichen Vereinbarung zwischen Ihnen und diesem Nutzer fertigen, dürfen Sie nur von zwei Anforderungen abweichen: der sicheren Standardkonfiguration (eine Rückkehr in einen sicheren Ausgangszustand muss möglich bleiben) und der unentgeltlichen Sicherheitsupdates (die Vereinbarung darf eine andere kommerzielle Grundlage festlegen). Alles Übrige gilt vollständig: Schwachstellenmanagement, die anderen Anforderungen an die Produktsicherheit, Meldungen nach Artikel 14, technische Dokumentation, CE-Kennzeichnung, Konformitätsbewertung und der Supportzeitraum. Dies ist keine allgemeine B2B-Ausnahme; sie deckt keine Standardprodukte ab, die an Unternehmen verkauft werden.





Die Produktklassifizierung bestimmt den Bewertungsweg

Ihre Produktkategorie bestimmt, wie Sie Konformität nachweisen.

Kategorie	Beispiele	Konformitätsbewertung
Standard, „nicht klassifiziert"	Allgemeine Software und vernetzte Verbraucherprodukte, die nicht zu den wichtigen oder kritischen Kategorien zählen	Modul A: Selbstbewertung

Kategorie	Beispiele	Konformitätsbewertung
Wichtig, „Klasse I"	Identitäts- und Zugriffsmanagement, Browser, Passwortmanager, Virenschutz, VPN, Netzwerkmanagement, Router, smarte Türschlösser, Sicherheitskameras und vergleichbare Produkte	Modul A nur, wenn anwendbare harmonisierte Normen, gemeinsame Spezifikationen oder Zertifizierungssysteme wie erforderlich angewandt werden; sonst Modul B+C oder Modul H
Wichtig, „Klasse II"	Hypervisoren, Container-Laufzeitumgebungen, Firewalls, IDS/IPS und manipulationsresistente Mikroprozessoren	Modul B+C, Modul H oder ein anwendbares europäisches Cybersicherheitszertifizierungssystem mindestens auf Vertrauenswürdigkeitsstufe „substanziell"
Kritische Produkte	Sichere Elemente, Smartcards, Smart-Meter-Gateways und Hardware-Sicherheitsboxen	Europäische Cybersicherheitszertifizierung, wenn erforderlich und verfügbar; sonst gelten die Wege der Klasse II

Die vier Produktkategorien

Die obige Tabelle zeigt Beispiele. Die vollständige Referenz, gegen die Sie die Kernfunktionalität Ihres Produkts vergleichen, ist nachfolgend dargestellt.

Standardprodukte

Die meisten Produkte landen hier. Jedes Produkt mit digitalen Elementen, dessen Kernfunktionalität nicht zu einem Eintrag auf den unten stehenden Listen für wichtige oder kritische Produkte passt, wird als Standardprodukt behandelt. Der Konformitätsweg ist die Selbstbewertung nach Modul A.

Häufige Beispiele:

- Smart-TVs und Streaming-Geräte.
- Netzwerkdrucker und Multifunktionsbürogeräte.
- Bluetooth-Lautsprecher und Audioprodukte für Verbraucher.
- Anwendungen für Mediaplayer.
- Spielkonsolen, E-Reader und ähnliche Unterhaltungselektronik.
- Smarte Küchengeräte wie Backöfen, Kühlschränke und Geschirrspüler ohne Sicherheitsfunktionen.
- Smarte Glühbirnen und vernetzte Beleuchtung ohne Sicherheitsfunktionen.
- Fitness-Tracker ohne Gesundheitsüberwachungszweck.
- Allgemeine Mobilanwendungen, die keine Browser, Passwortmanager oder VPN-Apps sind.
- Bürosoftware wie Textverarbeitung und Tabellenkalkulation.

Die obige Liste ist illustrativ. Die nachfolgenden Listen für wichtige und kritische Produkte sind abschließend.

Wichtige Produkte (Klasse I)

Verpflichtende Drittprüfung, sofern nicht anwendbare harmonisierte Normen, gemeinsame Spezifikationen oder Zertifizierungssysteme wie erforderlich angewandt werden.

1. Software und Hardware für Identitätsmanagement und Privileged Access Management, einschließlich Authentifizierungs- und Zutrittskontrollleser (einschließlich biometrischer Leser).
2. Eigenständige und eingebettete Browser.
3. Passwortmanager.
4. Software, die nach schädlicher Software sucht, sie entfernt oder in Quarantäne stellt.
5. VPN-Produkte.
6. Netzwerkmanagementsysteme.
7. Systeme für Security Information and Event Management (SIEM).
8. Bootmanager.
9. Software für Public-Key-Infrastrukturen und die Ausstellung digitaler Zertifikate.
10. Physische und virtuelle Netzschnittstellen.
11. Betriebssysteme.
12. Router, Modems für die Verbindung mit dem Internet und Switches.
13. Mikroprozessoren mit sicherheitsbezogenen Funktionen.

14. Mikrocontroller mit sicherheitsbezogenen Funktionen.
15. ASICs und FPGAs mit sicherheitsbezogenen Funktionen.
16. Smart-Home-Allzweckassistenten.
17. Smart-Home-Produkte mit Sicherheitsfunktionen (smarte Türschlösser, Sicherheitskameras, Babyphones, Alarmanlagen).
18. Internetfähiges Spielzeug mit interaktiven Funktionen (Sprechen, Filmen, Standortverfolgung).
19. Persönliche Wearables mit Gesundheitsüberwachungszweck (sofern nicht Verordnung (EU) 2017/745 oder 2017/746 greift) oder Wearables, die für die Nutzung durch Kinder bestimmt sind.

Wichtige Produkte (Klasse II)

Verpflichtende Drittprüfung, strengerer Weg. Selbstbewertung steht auch dann nicht offen, wenn harmonisierte Normen vorhanden sind.

1. Hypervisoren und Container-Laufzeitsysteme, die die virtualisierte Ausführung von Betriebssystemen und vergleichbaren Umgebungen unterstützen.
2. Firewalls, Systeme zur Erkennung und Verhinderung von Eindringversuchen.
3. Manipulationsresistente Mikroprozessoren.
4. Manipulationsresistente Mikrocontroller.

Kritische Produkte

Europäische Cybersicherheitszertifizierung erforderlich, wenn das Schema verfügbar ist. Sonst gilt der Weg der Klasse II.

1. Hardwaregeräte mit Sicherheitsboxen.
2. Smart-Meter-Gateways in intelligenten Messsystemen im Sinne des Artikels 2 Nummer 23 der Richtlinie (EU) 2019/944 sowie andere Geräte für fortgeschrittene Sicherheitszwecke, einschließlich der sicheren Kryptoverarbeitung.
3. Smartcards und ähnliche Geräte, einschließlich sicherer Elemente.

Wenn die Kernfunktionalität Ihres Produkts zu einem Eintrag auf den Listen für wichtige oder kritische Produkte passt, sind Sie in dieser Klasse. Wenn Ihr Produkt einen solchen Eintrag als Komponente integriert, seine eigene Kernfunktionalität aber etwas anderes ist, ändert die Integration Ihre Klasse nicht).

So klassifizieren Sie richtig: Kernfunktionalität, nicht Integration

Die obigen Listen sagen Ihnen, welche Kategorien es gibt. Sie sagen Ihnen nicht, wie Sie diese auf Ihr Produkt anwenden. Die Antwort der CRA ist ein Begriff: **Kernfunktionalität**.

Ihre Klasse ergibt sich daraus, was die Kernfunktionalität Ihres Produkts ist, nicht daraus, welche Komponenten es integriert. Passt die Kernfunktionalität zu den Listen für wichtige Produkte, ist das Produkt wichtig (Klasse I oder Klasse II). Passt sie zur Liste der kritischen Produkte, ist das Produkt kritisch. Passt sie zu keiner, ist das Produkt ein Standardprodukt. Das ist der gesamte Test und 8(1)).

Die praktische Absicherung steckt im zweiten Satz von Artikel 7(1). Die Integration einer wichtigen Komponente verschiebt das integrierende Produkt nicht in die wichtige Klasse. Wenn Sie eine Firewall-Bibliothek in einen Smart-Home-Hub einbetten, wird der Hub dadurch nicht zur Firewall. Erwägungsgrund 45 bringt es auf den Punkt: Firewalls und Systeme zur Erkennung von Eindringversuchen sind wichtige Produkte der Klasse II, doch andere Produkte, die solche Komponenten zufällig integrieren, sind es nicht.

Nutzen Sie diese Reihenfolge zur Selbstklassifizierung.

1. **Benennen Sie die Kernfunktionalität Ihres Produkts in einem Satz.** Wenn Ihnen das nicht gelingt, scheitert die weitere Analyse. Konzentrieren Sie sich darauf, was das Produkt ohne diese Funktion nicht mehr leisten würde.
2. **Prüfen Sie die obigen Listen für wichtige Produkte.** Ein Treffer in Klasse I oder II macht das Produkt zu einem wichtigen Produkt.
3. **Prüfen Sie die obige Liste für kritische Produkte.** Ein Treffer macht das Produkt zu einem kritischen Produkt. Der europäische Cybersicherheitszertifizierungsweg gilt, wenn das Schema verfügbar ist; sonst gilt der Weg der Klasse II.
4. **Kein Treffer auf einer der Listen.** Das Produkt ist ein Standardprodukt. Der Weg ist die Selbstbewertung nach Modul A.
5. **Dokumentieren Sie die Begründung.** Ein einseitiger Vermerk mit der Aussage zur Kernfunktionalität, der Listenprüfung und dem gewählten Weg gehört in die technische Dokumentation.

Zwei konkrete Beispiele.

Smart-Home-Hub mit eingebettetem Passwortmanager. Kernfunktionalität: das Orchestrieren von Abläufen über vernetzte IoT-Geräte im Haushalt. Die Passwortmanager-Komponente, die ihr eigener Hersteller separat vertreibt, ist für sich genommen ein wichtiges Produkt der Klasse I. Die Kernfunktionalität des Hubs ist Heimautomation, nicht Anmeldedatenverwaltung. Der Hub bleibt ein Standardprodukt.

Betriebssystem nach Funktionsumfang. Ein Produkt wird als Smart-Home-Gerät vermarktet, doch seine Hauptfunktionen sind Hardware- und Peripherie-Initialisierung, Prozess-Scheduling, Speicherverwaltung und eine Systemaufrufschnittstelle. Das ist die Kernfunktionalität eines Betriebssystems. Betriebssysteme sind ein wichtiges Produkt der Klasse I. Das Produkt ist wichtig (Klasse I), unabhängig von der Vermarktung.

Wenn Ihre Klassifizierung in einer Klasse landet, die das übrige Team überrascht, braucht die Aussage zur Kernfunktionalität einen weiteren Durchgang, bevor Sie ausliefern.

Wenn die Cloud Teil Ihres Produkts ist

Die meisten Produkte mit digitalen Elementen stützen sich auf etwas, das nicht auf dem Gerät selbst läuft: ein Cloud-Backend, eine mobile Begleit-App, einen Server für Over-the-Air-Updates, ein Authentifizierungsportal, ein Gerätemanagementsystem. Die CRA behandelt nicht alles davon als Ihr Produkt. Sie zählt es nur dann zum Produkt, wenn **beide** Bedingungen erfüllt sind):

- Die Software wurde **von Ihrem Team oder unter Ihrer Verantwortung entworfen und entwickelt**.
- Das Produkt **könnte eine seiner Funktionen ohne sie nicht erfüllen**.

Wenn eine der Bedingungen nicht erfüllt ist, liegt der entfernte Dienst außerhalb der CRA-Produktgrenze. Ein Drittanbieter-SaaS, der Ihnen nicht gehört und mit dem Ihr Produkt lediglich kommuniziert, ist nicht Teil Ihres Produkts. Eine Website, die das Produkt bewirbt, aber keine seiner Funktionen unterstützt, ist ebenfalls nicht Teil des Produkts.

Wenn eine entfernte Komponente in den Anwendungsbereich fällt, fällt sie **als Teil des Produkts** hinein. Technische Dokumentation, Konformitätsbewertung, Konformitätserklärung, Schwachstellenmanagement und die Meldefristen nach Artikel 14 erfassen die Cloud-Komponente gemeinsam mit dem Gerät.

Nutzen Sie diese Matrix, um den Fall schnell zu klären.

Komponente	Als Teil des Produkts im Anwendungsbereich?
Mobile Begleit-App, die das Gerät koppelt	**Ja.** Sie haben sie entworfen, und das Gerät lässt sich ohne sie weder einrichten noch nutzen.
Cloud-Backend, das die Daten des Geräts speichert und verarbeitet	**Ja.** Sie haben es entworfen, und das Dashboard oder die Hauptfunktion arbeitet ohne es nicht.
Server für Over-the-Air-Updates	**Ja.** Sie haben ihn entworfen, und das Gerät kann ohne ihn keine Sicherheitsupdates empfangen.
Authentifizierungsportal, das den Zugriff auf das Gerät steuert	**Ja.** Sie haben es entworfen, und Nutzer können sich ohne es nicht anmelden.
Marketingwebsite für das Produkt	**Nein.** Sie unterstützt keine Produktfunktion.
Drittanbieter-SaaS, mit dem das Produkt integriert ist (gehört Ihnen nicht)	**Nein.** Nicht von Ihnen entworfen. Der Drittanbieter trägt seine eigenen Pflichten nach NIS 2.
Generische Cloud-Infrastruktur, auf der Ihr Dienst läuft (IaaS oder PaaS)	**Nein.** Nicht von Ihnen entworfen. Der Infrastrukturanbieter fällt unter NIS 2.

Ein häufiges Muster: ein Smart-Home-Gerät mit einer mobilen App, einem Update-Server und einem Cloud-Backend. Alle drei sind vom Hersteller entworfen, und das Gerät kann seine beworbenen Funktionen ohne sie nicht erbringen. Alle drei sind Teil des Produkts. Die CRA-Pflichten gelten für das gesamte Paket. Wenn das Cloud-Backend dann mit einem Drittanbieter-SaaS für Analytics kommuniziert, ist dieser SaaS nicht Teil des Produkts. Der Drittanbieter trägt seine eigenen Pflichten nach NIS 2.

Die CRA verlangt keine Sicherheitsmaßnahmen für die Netz- und Informationssysteme des Herstellers insgesamt. Sie verlangt Sicherheit für die entfernten Dienste, die Teil des Produkts sind. Die Grenze ist die Produktgrenze, nicht die Unternehmensgrenze.

Ihre Lieferkette: wer macht was unter dem CRA

Der CRA legt die Hauptpflichten auf Sie als Hersteller, doch auch Einführer und Händler tragen Pflichten, die darauf wirken, wie Ihr Produkt auf den Markt gelangt. Drei Dinge sollten Sie wissen.

Wer	Was sie vor der Lieferung prüfen	Was sie bei einer Schwachstelle tun	Wann sie Ihre Pflichten übernehmen
Einführer	CE-Kennzeichnung, EU-Konformitätserklärung, Benutzerinformationen in der richtigen Sprache, Ihre Kontaktdaten auf oder mit dem Produkt	Informieren Sie unverzüglich; informieren Marktüberwachungsbehörden direkt, wenn das Produkt ein erhebliches Cybersicherheitsrisiko darstellt	Wenn sie Ihr Produkt unter ihrem eigenen Namen oder Markenzeichen in Verkehr bringen oder es wesentlich verändern
Händler	CE-Kennzeichnung, dass Sie und der Einführer Ihren Teil getan haben, dass die erforderlichen Dokumente das Produkt begleiten	Informieren Sie unverzüglich; informieren Marktüberwachungsbehörden direkt, wenn das Produkt ein erhebliches Cybersicherheitsrisiko darstellt; können die Bereitstellung stoppen	Gleicher Auslöser wie bei Einführern

Für einen Hersteller bedeutet das drei praktische Punkte:

- Ihre CE-Kennzeichnung, Ihre EU-Konformitätserklärung und Ihre Benutzerinformationen müssen in dem Moment korrekt und in der richtigen Sprache vorliegen, in dem ein Händler sie prüft. Vertriebspartner sind verpflichtet, diese zu verifizieren, und können die Bereitstellung verweigern, wenn etwas fehlt oder fehlerhaft ist.
- Sie benötigen einen klaren, niedrigschwelligen Kontaktweg, über den Einführer und Händler Schwachstellen in Ihren Prozess für das Schwachstellenmanagement einspeisen können. Sie werden ihn nutzen.
- Jeder Partner, der Ihr Produkt umetikettiert, unter eigenem Namen oder Markenzeichen in Verkehr bringt oder wesentlich verändert, wird zum Hersteller dieser Variante. Die vollständigen Pflichten zu technischer Dokumentation, Konformitätsbewertung, Meldungen und Supportzeitraum gehen für diese Version auf ihn über. Siehe *Wenn jemand anderes zum Hersteller wird* im nächsten Abschnitt für die Regel zur wesentlichen Änderung.

Wesentliche Änderung: wann eine erneute Konformität erforderlich ist

Nach dem Inverkehrbringen Ihres Produkts teilt der CRA spätere Änderungen in zwei Lager. Die meisten sind Routine und brauchen nichts Zusätzliches. Manche sind wesentlich. Eine wesentliche Änderung wird für Zwecke des CRA so behandelt, als würde ein neues Produkt in Verkehr gebracht. Das bedeutet eine neue Konformitätsbewertung, eine aktualisierte technische Dokumentation, eine neue Konformitätserklärung und eine CE-Kennzeichnung auf der neuen Version.

Der Test ist kurz und steht in der Begriffsbestimmung der wesentlichen Änderung). Eine Änderung ist wesentlich, wenn eines der beiden Kriterien zutrifft:

- Sie **wirkt sich auf die Konformität** mit den grundlegenden Cybersicherheitsanforderungen aus.
- Sie **verändert den bestimmungsgemäßen Zweck**, für den das Produkt geprüft wurde.

Wenn keines zutrifft, ist die Änderung nicht wesentlich. Dokumentieren Sie die Begründung trotzdem und legen Sie sie ab. Die Analyse gehört zur Nachweiskette.

Was nicht als wesentlich gilt

Zwei Ausnahmen leisten in der Praxis die meiste Arbeit.

Sicherheitsupdates und Fehlerbehebungen, die das Cybersicherheitsrisiko verringern, ohne den bestimmungsgemäßen Zweck zu ändern, sind nicht wesentlich. Das Patchen einer bekannten Schwachstelle, das Anpassen einer Eingabevalidierung zur Schließung eines Fehlers oder das Neubauen einer Komponente zur Behebung einer CVE liegen alle auf dieser Seite der Linie.

Wiederaufarbeitung, Wartung und Reparaturen sind ebenfalls nicht automatisch wesentlich. Sie werden nur dann wesentlich, wenn sie den bestimmungsgemäßen Zweck verändern oder die Konformität mit den grundlegenden Cybersicherheitsanforderungen beeinflussen.

Kleinere Arbeiten an der Benutzeroberfläche bleiben ebenfalls auf der sicheren Seite. Eine Sprache hinzuzufügen, einen Icon-Satz auszutauschen oder ein Bildschirmlayout zu polieren ist für sich genommen keine wesentliche Änderung. Das Hinzufügen eines neuen Eingabeelements, das eine angemessene Eingabevalidierung erfordert, kann es jedoch sein.

Ersatzteile

Der CRA nimmt Ersatzteile auf eine eng umrissene Weise aus. **Identische Ersatzteile**, die nach denselben Spezifikationen wie die ersetzten Komponenten gefertigt sind, fallen vollständig aus dem Anwendungsbereich der Verordnung. Funktional gleichwertige Ersatzteile nicht.

Nutzen Sie diese Matrix, um den Fall schnell zu klären.

Ersatzteil	Wirtsprodukt vor dem 11. Dezember 2027 in Verkehr gebracht	Wirtsprodukt ab dem 11. Dezember 2027 in Verkehr gebracht
Identisch zur Originalkomponente, gleiche Spezifikationen	Ersatzteil außerhalb des CRA-Anwendungsbereichs. Der Austausch löst keine Pflichten aus.	Ersatzteil außerhalb des CRA-Anwendungsbereichs. Der Austausch löst keine Pflichten aus.
Funktional gleichwertig, abweichendes Design oder abweichende Spezifikation	Das Ersatzteil ist ein eigenständiges CRA-Produkt. Das Wirtsprodukt hat keine CRA-Pflichten, da es vor dem Anwendungsdatum liegt.	Das Ersatzteil ist ein CRA-Produkt. Prüfen Sie mit dem zweistufigen Test oben, ob der Einbau in das Wirtsprodukt eine wesentliche Änderung des Wirtsprodukts darstellt.

Zwei praktische Folgen. Erstens hängt die Ausnahme von identischen Spezifikationen ab. Ein Funkmodul, das auf einem anderen Chipsatz neu gebaut wurde, ist kein identisches Ersatzteil, auch wenn Kundinnen und Kunden den Unterschied nicht bemerken. Zweitens trägt der Hersteller, der einen funktional gleichwertigen Ersatz liefert, die CRA-Pflichten für dieses Teil, unabhängig davon, wer das Wirtsprodukt hergestellt hat.

Software-Updates und Feature-Flags

Software-Releases sind die häufigste Quelle für Fragen zur wesentlichen Änderung. Der zweistufige Test klärt sie auch hier.

Ein Patch, der eine Schwachstelle behebt, ist nicht wesentlich. Ein Feature-Schalter, der eine Fähigkeit aktiviert, für die das Produkt nie geprüft wurde, ist es. Ein Modell-Upgrade, das dem Produkt erlaubt, über neue Kategorien von Eingaben zu entscheiden, ebenfalls. Wenn ein Release sowohl eine Fehlerbehebung als auch eine neue Funktion enthält, bewerten Sie die neue Funktion.

Bündelung zählt weniger als der Gehalt. Ob ein Funktionsupdate allein oder im selben Release wie ein Sicherheitspatch ausgeliefert wird, ist für die Bewertung unerheblich.

Wenn Sie Feature-Flags oder gestaffelte Rollouts betreiben, zählt der Moment der Aktivierung für Endnutzerinnen und Endnutzer in der Produktion, nicht das Ausliefern des Binaries, das den Schalter enthält.

Die Entscheidung in der Praxis

Nutzen Sie diese Reihenfolge bei jeder Änderung, bevor Sie ausliefern.

1. **Verändert die Änderung den bestimmungsgemäßen Zweck des Produkts?** Wenn ja: wesentlich. Führen Sie die Konformitätsbewertung für die neue Version erneut durch.
2. **Wirkt sich die Änderung auf die Konformität mit den grundlegenden Cybersicherheitsanforderungen aus?** Wenn ja: wesentlich. Führen Sie die Konformitätsbewertung für die neue Version erneut durch.
3. **Andernfalls:** nicht wesentlich. Dokumentieren Sie die Analyse und arbeiten Sie unter der bestehenden technischen Dokumentation weiter.

Wenn das Produkt zur Klasse der wichtigen oder kritischen Produkte zählt und der Weg beim ersten Mal eine Drittprüfung verlangte, bringt eine wesentliche Änderung Sie zurück auf denselben Weg. Benachrichtigen Sie die dritte Stelle frühzeitig über jede Änderung, die wahrscheinlich wesentlich ist. Selbstbewertung ist kein Hintertürchen, um ein wichtiges Produkt im Nachhinein neu zu klassifizieren.

Folgen, wenn eine Änderung wesentlich ist

Eine wesentliche Änderung wird so behandelt, als würde ein neues Produkt in Verkehr gebracht. Für den Hersteller heißt das:

- Aktualisieren Sie die technische Dokumentation für die geänderte Version.
- Führen Sie die Konformitätsbewertung entlang des Wegs erneut durch, den die Produktklasse verlangt.
- Stellen Sie eine neue EU-Konformitätserklärung für die geänderte Version aus.
- Bringen Sie die CE-Kennzeichnung erneut an, mit der neuen Erklärung in der Akte.
- Bewahren Sie die Dokumentation der vorherigen Version für die volle Aufbewahrungsfrist. Die neue Version löscht sie nicht.

Insbesondere bei Softwareprodukten können Sie Sicherheitsupdates während des Supportzeitraums auf die jeweils neueste in Verkehr gebrachte Version beschränken, sofern Nutzerinnen und Nutzer früherer Versionen kostenfrei und ohne neue Hardware auf die neueste Version wechseln können.

Bereits verkaufte Feldgeräte mit der vorherigen Konformität bleiben unberührt. Die Pflicht knüpft an die bereitgestellte geänderte Version an, nicht an identische Einheiten, die zeitlich vorher liegen.

Wenn jemand anderes zum Hersteller wird

Wenn Sie nicht der ursprüngliche Hersteller sind und eine wesentliche Änderung vornehmen, behandelt der CRA Sie als Hersteller dieser Version. Die vollständigen Pflichten der Artikel 13 und 14 treffen Sie. Dieselbe Regel gilt, wenn Sie das Produkt unter Ihrem eigenen Namen oder Markenzeichen in Verkehr bringen.

Das erfasst mehr Konstellationen als Teams üblicherweise erwarten:

- Eine Systemintegrationsfirma, die einen kundenspezifischen Firmware-Build mit neuen Funktionen ausliefert.
- Ein Wiederverkäufer, der ein Produkt umlabelt und den vermarkteten bestimmungsgemäßen Zweck ändert.
- Ein Dienstleister, der ein Gerät eines Drittanbieters mit eigener Firmware bündelt.

In jedem Fall übernimmt der Akteur, der die Änderung vorgenommen hat, die Herstellerpflichten für diese Version: technische Dokumentation, Konformitätsbewertung, Meldungen, Schwachstellenmanagement und alles Übrige. Das Etikett „Einführer" oder „Händler" schützt ab dem Moment, in dem eine der Linien überschritten wird, nicht mehr.

Was Sie bereithalten müssen

Nutzen Sie diesen Abschnitt als Arbeitscheckliste. Die detaillierte Anleitung zu jeder Anforderung folgt danach.

Cybersicherheits-Risikobewertung

Vor dem Inverkehrbringen eines Produkts benötigen Sie eine Cybersicherheits-Risikobewertung in der Akte. Sie ist das Dokument, das in Ihren eigenen Worten erklärt, warum das Produkt sicher in Verkehr gebracht und am Markt gehalten werden kann.

Die Bewertung sollte abdecken:

- Den bestimmungsgemäßen Zweck des Produkts und die Anwendungsfälle, die Sie vernünftigerweise vorhersehen können
- Die Bedingungen und die Umgebung, in der das Produkt betrieben wird
- Die Daten und Funktionen, die geschützt werden müssen
- Die einschlägigen Bedrohungen und die Schutzmaßnahmen, auf die Sie sich stützen
- Die Zeitspanne, über die das Produkt voraussichtlich genutzt wird

So strukturieren die meisten Teams ihre Bewertung. Belastbare Methoden konvergieren auf dieselben Schritte: die Werte identifizieren (Daten, die das Produkt verarbeitet, Sicherheitsmaterial wie Schlüssel und Anmeldedaten, Funktionen, deren Verlust Nutzerinnen und Nutzern schaden würde), abbilden, wo jeder Wert liegt oder sich bewegt, die Bedrohungen je Wert und Umgebung entlang Vertraulichkeit, Integrität und Verfügbarkeit modellieren, Auswirkung und Eintrittswahrscheinlichkeit bewerten, entscheiden, welche Restrisiken akzeptiert und welche gemindert werden, und nach jeder Runde Schutzmaßnahmen neu bewerten (jeder neue Schlüssel, jedes neue Zertifikat und jede neue Authentifizierungsfunktion ist ihrerseits ein neuer Wert, der zu analysieren ist).

Threat Modelling. Schritt drei oben ist der technisch anspruchsvollste und hat eigene etablierte Techniken. STRIDE kategorisiert Bedrohungen als Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service und Elevation of Privilege; weit verbreitet, passt für die meisten vernetzten Produkte. LINDDUN erweitert das Bild für Produkte, die personenbezogene Daten verarbeiten, um Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of Information, Unawareness und Non-compliance; nützlich dort, wo sich das Datenschutzregime mit CRA-Pflichten überschneidet. PASTA führt einen siebenstufigen Prozess von den Geschäftszielen bis zur Akzeptanz von Restrisiken; nützlich für komplexe Systeme, in denen das Angriffsbild das Design treibt. Keines davon ist CRA-spezifisch, und der CRA verlangt keines im Besonderen. Wählen Sie das, was zum Expositionsprofil Ihres Produkts passt.

Wo Sie eine ausgearbeitete Methodik finden. Der CRA schreibt keine Methode vor. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht mit der Technischen Richtlinie TR-03183 die detaillierteste öffentlich verfügbare, an der CRA ausgerichtete Methodik für Risikobewertungen. ENISA veröffentlicht breiter angelegte CRA-Umsetzungsleitlinien.

Halten Sie die Bewertung während des gesamten Supportzeitraums aktuell. Wenn sich Bedrohungsbild, Komponenten oder Anwendungsfall ändern, sollte sich die Bewertung mit ihnen ändern.

Festlegung des Supportzeitraums

Jedes Produkt benötigt einen festgelegten Supportzeitraum, und Sie müssen sein Enddatum zum Zeitpunkt des Kaufs veröffentlichen. Der Supportzeitraum ist die Spanne, in der Sie Schwachstellen bearbeiten, Sicherheitsupdates ausliefern und die technische Dokumentation aktuell halten.

Wie lang er sein muss

Mindestens fünf Jahre. Wird das Produkt voraussichtlich weniger als fünf Jahre genutzt, muss der Supportzeitraum der erwarteten Nutzungsdauer entsprechen. Wird es länger genutzt, muss der Supportzeitraum diese längere Nutzung abbilden; Produkte wie Router, Betriebssysteme und industrielle Steuerungen rechtfertigen routinemäßig mehr als fünf Jahre.

Welche Faktoren in Betracht zu ziehen sind

Berücksichtigen Sie bei der Festlegung des Zeitraums verhältnismäßig:

- Vernünftige Nutzererwartungen an das Produkt
- Die Art des Produkts, einschließlich des bestimmungsgemäßen Zwecks
- Jedes EU-Recht, das für diese Produktkategorie bereits eine Lebensdauer vorsieht
- Supportzeiträume vergleichbarer Produkte am Markt
- Die Verfügbarkeit der Betriebsumgebung, auf die das Produkt angewiesen ist
- Die Supportzeiträume integrierter Komponenten, die zentrale Funktionen liefern
- Etwaige Leitlinien der ADCO oder der Kommission für die Produktkategorie

Die Begründung des gewählten Zeitraums muss in der technischen Dokumentation stehen. Marktüberwachungsbehörden können sie anfordern.

Was Sie veröffentlichen müssen

Geben Sie das Ende des Supportzeitraums zum Zeitpunkt des Kaufs an, mindestens mit Monat und Jahr, an einer leicht zugänglichen Stelle. Verfügt das Produkt über eine Benutzeroberfläche, zeigen Sie eine Benachrichtigung an, wenn es das Ende seines Supportzeitraums erreicht.

Aufbewahrung von Updates

Jedes während des Supportzeitraums den Nutzerinnen und Nutzern bereitgestellte Sicherheitsupdate muss mindestens 10 Jahre nach seiner Bereitstellung verfügbar bleiben oder für den Rest des Supportzeitraums, je nachdem, welcher Zeitraum länger ist.

Komponenten-Due-Diligence

Ein Produkt besteht aus Komponenten. Manche haben Sie geschrieben, manche zugekauft, manche aus einem Open-Source-Repository gezogen. Der CRA behandelt das Produkt für die Compliance als Ganzes, also zählen auch die Komponenten. Sitzt eine Schwachstelle in einer Komponente, sitzt sie in Ihrem Produkt. Erhält eine Komponente keine Sicherheitsupdates, erhält auch Ihr Produkt keine.

Hersteller müssen Drittanbieterkomponenten einer Sorgfaltsprüfung unterziehen, einschließlich freier und quelloffener Komponenten. Die Komponenten dürfen die Cybersicherheit des Produkts nicht beeinträchtigen.

Wie viel Sorgfalt ausreicht, hängt vom Cybersicherheitsrisiko der Komponente ab. Eine Bibliothek, die Authentifizierung handhabt, ist nicht dasselbe wie eine Bibliothek für die Schriftartendarstellung. Nutzen Sie eine oder mehrere der folgenden Prüfungen, verhältnismäßig zum Risiko:

1. **Prüfen Sie die CE-Kennzeichnung der Komponente.** Wenn die Komponente selbst ein CRA-Produkt ist und der Lieferant Konformität nachgewiesen hat, trägt die Komponente die CE-Kennzeichnung. Das belegt die CRA-Arbeit des Lieferanten.
2. **Prüfen Sie die Historie der Sicherheitsupdates.** Eine Komponente, die regelmäßig Sicherheitsupdates erhält, ist ein besseres Risiko als eine, die seit Jahren stillsteht. Achten Sie auf einen Release-Rhythmus und auf eine jüngere Historie von Sicherheits-Advisories.
3. **Prüfen Sie die Komponente gegen Schwachstellendatenbanken.** Die europäische Schwachstellendatenbank und öffentliche CVE-Datenbanken zeigen, was über die Komponente bekannt ist. Eine bekannte CVE ohne Patch ist ein Warnsignal.
4. **Führen Sie weitere Sicherheitstests durch.** Wo das oben Genannte nicht reicht, testen Sie die Komponente in Ihrem Integrationskontext: statische Analyse, dynamische Analyse, Fuzzing oder ein gezielter Sicherheitsreview.

Für Komponenten, die integriert werden, bevor ihr eigener Lieferant vollständig unter dem CRA steht (sodass noch keine CE-Kennzeichnung verfügbar ist), nutzen Sie stattdessen die anderen drei Prüfungen. Die Sorgfaltspflicht pausiert nicht, weil die Lieferkette noch aufholt.

Nachweise, die in der Akte liegen müssen

Die technische Dokumentation muss Ihre Sorgfalt zeigen, nicht nur behaupten. Bewahren Sie auf:

- Eine Liste der im Produkt enthaltenen Drittanbieterkomponenten, nachvollziehbar bis auf die Version, einschließlich Open-Source. Die SBOM ist hierfür der natürliche Ort.
- Die Sicherheitsdokumentation der Lieferanten, die Sie geprüft haben: Sicherheitsrichtlinien, Programme zur Offenlegung von Schwachstellen, Zusagen zum Supportzeitraum.
- Integrationstest-Berichte, die zeigen, dass die Komponente sich in Ihrem Produkt sicher verhält.
- Sicherheitsklauseln in Verträgen oder SLAs mit kommerziellen Lieferanten: Fristen für Schwachstellenbenachrichtigungen, Zusagen zum Supportzeitraum, Eskalationsregeln.
- Aufzeichnungen über die Schutzmaßnahmen auf Produktebene, die Sie dort ergänzt haben, wo die Komponenten-Due-Diligence Grenzen offenbart hat: Sandboxing, eingeschränkte Berechtigungen, Eingabevalidierung, Netzsegmentierung.

Wenn Sie eine Schwachstelle in einer Komponente finden

Wenn Ihre Sorgfaltsprüfung oder Ihre Überwachung nach dem Inverkehrbringen eine Schwachstelle in einer Komponente identifiziert, müssen Sie zwei Dinge tun. Erstens: Benachrichtigen Sie die Person oder Einrichtung, die die Komponente pflegt. Bei Open Source ist das das Upstream-Projekt. Zweitens: Beheben und mindern Sie die Schwachstelle in Ihrem Produkt innerhalb derselben Fristen wie bei jeder anderen Schwachstelle, die Sie entdecken. Haben Sie eine Korrektur entwickelt, teilen Sie den Code oder die Dokumentation mit der Maintainer-Seite, sofern anwendbar in maschinenlesbarem Format.

Der CRA erlaubt es nicht, auf das Handeln der Komponenten-Maintainer zu warten, bevor Sie Ihre eigenen Nutzerinnen und Nutzer schützen. Die Frist für das Schwachstellenmanagement Ihres Produkts läuft unabhängig vom Upstream.

Die 13 Anforderungen an die Produktsicherheit

Jedes Produkt mit digitalen Elementen muss beim Inverkehrbringen dreizehn grundlegende Sicherheitsanforderungen erfüllen und während des gesamten Supportzeitraums erfüllen. Sie sind die Untergrenze dafür, was Cybersicherheit im Produktverständnis des CRA bedeutet.

Die dreizehn Anforderungen sind:

- Keine bekannten ausnutzbaren Schwachstellen zum Zeitpunkt des Inverkehrbringens
- Sichere Standardkonfiguration ab Werk
- Sicherheitsupdates, einschließlich automatischer Updates mit Opt-out
- Schutz vor unbefugtem Zugriff
- Vertraulichkeit gespeicherter, übertragener und verarbeiteter Daten
- Integrität von Daten, Firmware und Konfiguration
- Datenminimierung
- Verfügbarkeit und Resilienz, auch gegen Denial-of-Service-Angriffe
- Keine negativen Auswirkungen auf andere verbundene Geräte oder Netze
- Begrenzte Angriffsfläche, einschließlich externer Schnittstellen
- Verringerte Auswirkungen von Sicherheitsvorfällen durch Exploitation-Mitigation
- Protokollierung sicherheitsrelevanter Aktivitäten mit Opt-out für Nutzer
- Sichere und dauerhafte Datenlöschung und Portabilität

Jede Anforderung wird später im Leitfaden im Detail aufgeschlüsselt, samt praktischer Bedeutung und der Nachweise, die in der Akte liegen sollten.

Die 8 Anforderungen an das Schwachstellenmanagement

Hersteller benötigen außerdem Prozesse für das Schwachstellenmanagement, die während des gesamten Supportzeitraums des Produkts laufen:

1. Schwachstellen identifizieren und dokumentieren (einschließlich Software Bill of Materials, SBOM)
2. Risikomanagement und zeitnahe Sicherheitsupdates
3. Regelmäßige Sicherheitstests
4. Benachrichtigung über Sicherheitsupdates und Offenlegung von Schwachstellen
5. Strategie für die koordinierte Offenlegung von Schwachstellen (CVD)
6. Kontaktadresse für den Austausch und die Meldung von Schwachstellen
7. Sichere Mechanismen zur Verteilung von Updates
8. Kostenlose Sicherheitsupdates mit Hinweismeldungen

Meldefristen nach Artikel 14

Diese Pflichten gelten ab dem **11. September 2026**. Sie gelten für Hersteller von Produkten mit digitalen Elementen im Anwendungsbereich, einschließlich Produkten, die vor dem **11. Dezember 2027** in Verkehr gebracht wurden. Kleinstunternehmen und kleine Unternehmen sind von der Meldepflicht nicht generell ausgenommen. Die Bußgeld-Erleichterung für kleine Unternehmen ist eng begrenzt: Sie betrifft nur die erste **24-Stunden-Frist für die Frühwarnung**.

Der CRA unterscheidet drei Stufen des Schwachstellenstatus:

- **Schwachstelle:** jede Schwäche, die ausgenutzt werden könnte
- **Ausnutzbare Schwachstelle:** eine Schwäche, die unter realen Bedingungen genutzt werden kann
- **Aktiv ausgenutzte Schwachstelle:** eine Schwachstelle, deren Nutzung in einem Angriff bestätigt wurde

Wann die Uhr zu laufen beginnt

Sie sind nicht in dem Moment im Lauf, in dem ein Signal eingeht. Die Uhr beginnt zu laufen, sobald Sie eine erste Bewertung abgeschlossen haben und mit hinreichender Sicherheit davon ausgehen, dass eine Schwachstelle in Ihrem Produkt aktiv ausgenutzt wird oder dass ein schwerwiegender Vorfall die Sicherheit Ihres Produkts beeinträchtigt hat. Der Akzent liegt auf der zügigen Erstbewertung, nicht auf dem Warten auf den Abschluss der vollständigen Untersuchung. Wenn Kundinnen, Forschende, Behörden oder andere Dritte ein mögliches Problem an Sie herantragen, bewerten Sie es unverzüglich und starten Sie die Uhr, sobald diese Bewertung die hinreichende Sicherheit ergibt.

Wenn Sie eine **aktiv ausgenutzte Schwachstelle** erkennen, gilt die folgende Meldefrist:

Frist	Was erforderlich ist	Wo zu melden ist
Innerhalb von 24 Stunden	Frühwarnung über die aktive Ausnutzung	ENISA über nationales CSIRT
Innerhalb von 72 Stunden	Schwachstellenmeldung: betroffenes Produkt, allgemeine Art des Exploits und der Schwachstelle, Abhilfemaßnahmen, Korrekturmaßnahmen, die Nutzer ergreifen können, und Sensitivitätskennzeichnung, soweit anwendbar	ENISA über nationales CSIRT
Spätestens 14 Tage nachdem eine Korrektur- oder Minderungsmaßnahme verfügbar ist	Abschlussbericht: Beschreibung der Schwachstelle, Schweregrad, Auswirkungen, verfügbare Informationen zu böswilligen Akteuren und Details zum Sicherheitsupdate oder anderen Korrekturmaßnahmen	ENISA über nationales CSIRT

Wenn Sie einen **schwerwiegenden Sicherheitsvorfall** mit Auswirkungen auf die Sicherheit des Produkts erkennen, gilt die folgende Meldefrist:

Frist	Was erforderlich ist	Wo zu melden ist
Innerhalb von 24 Stunden	Frühwarnung, einschließlich der Angabe, ob der Vorfall mutmaßlich durch rechtswidrige oder böswillige Handlungen verursacht wurde	ENISA über nationales CSIRT
Innerhalb von 72 Stunden	Sicherheitsvorfallmeldung: Art des Vorfalls, erste Bewertung, Abhilfemaßnahmen, Korrekturmaßnahmen, die Nutzer ergreifen können, und Sensitivitätskennzeichnung, soweit anwendbar	ENISA über nationales CSIRT
Innerhalb eines Monats nach der 72-Stunden-Sicherheitsvorfallmeldung	Abschlussbericht: detaillierte Beschreibung des Sicherheitsvorfalls, Schweregrad, Auswirkungen, wahrscheinliche Bedrohung oder Ursache sowie angewandte oder laufende Minderungsmaßnahmen	ENISA über nationales CSIRT

Meldungen werden aktualisiert, wenn Sie mehr wissen

Die Einreichungen nach 24 Stunden, 72 Stunden und 14 Tagen (oder einem Monat) sind Stufen derselben Meldung, keine separaten Einreichungen. Jede Stufe ergänzt die Informationen, die in der vorherigen noch nicht verfügbar waren. Das als Koordinator bestimmte CSIRT kann jederzeit auch um eine Zwischenaktualisierung bitten. Sie müssen Informationen, die Sie bereits übermittelt haben, nicht wiederholen.

Meldungen werden über die **zentrale CRA-Meldeplattform** eingereicht und über das nationale Computer Security Incident Response Team (CSIRT) im Hauptmitgliedstaat des Herstellers geroutet, mit gleichzeitigem Zugriff für ENISA.

Ihre Nutzerinnen und Nutzer informieren

Nach Kenntnisnahme müssen Sie die betroffenen Nutzerinnen und Nutzer und, sofern angemessen, alle Nutzerinnen und Nutzer über die Schwachstelle oder den Vorfall sowie über Risikominderungs- und Korrekturmaßnahmen informieren, die sie selbst anwenden können. Das ist nicht dasselbe wie eine öffentliche Offenlegung. Die Pflicht besteht darin, die Informationen verhältnismäßig zum Risiko an die Nutzerinnen und Nutzer zu bringen, die sie zu ihrem Schutz brauchen. Bei Produkten in sensiblen oder wesentlichen Umgebungen beschränken Sie detaillierte technische Informationen auf die betroffenen Kundinnen und Kunden, solange die Schwachstelle nicht gemindert ist; vorzeitige öffentliche Details können die Ausnutzung erleichtern.

Sobald die Schwachstelle behoben oder gemindert ist, kann eine breitere Offenlegung angemessen werden, damit Nutzerinnen und Nutzer prüfen können, dass ihre Produkte nicht mehr betroffen sind, und damit das allgemeine Bewusstsein steigt. Halten Sie Detailgrad und Zeitpunkt verhältnismäßig zum Restrisiko. Informieren Sie Nutzerinnen und Nutzer nicht rechtzeitig, kann das CSIRT einspringen und die Informationen selbst bereitstellen, wenn es das für verhältnismäßig und erforderlich hält.

Aktiv ausgenutzte Schwachstelle	
24 Stunden	Frühwarnung
72 Stunden	Schwachstellenmeldung
14 Tage nach Korrekturmaßnahme	Abschlussbericht

Schwerwiegender Sicherheitsvorfall	
24 Stunden	Frühwarnung
72 Stunden	Sicherheitsvorfallmeldung
ein Monat nach 72-Stunden-Meldung	Abschlussbericht

Korrekturmaßnahmen, wenn ein Produkt nicht konform ist

Wenn Sie wissen oder Anlass zu der Annahme haben, dass ein von Ihnen in Verkehr gebrachtes Produkt oder einer Ihrer Prozesse nicht den grundlegenden Cybersicherheitsanforderungen des CRA entspricht, müssen Sie unverzüglich handeln. Die Pflicht läuft ab dem Inverkehrbringen und für den gesamten Supportzeitraum.

Die drei Optionen

1. **In Konformität bringen.** Beheben Sie das Produkt oder den Prozess. Für Softwareprodukte ist das in der Regel ein Sicherheitsupdate oder eine Prozessänderung. Wenden Sie die Korrektur auf die unterstützten Versionen an.
2. **Vom Markt nehmen.** Stellen Sie die Bereitstellung am Markt ein. Ziehen Sie es aus Ihrer Lieferkette und aus Lager, Integrationen und Wiederverkauf zurück.
3. **Rückrufen.** Holen Sie das Produkt von Nutzerinnen und Nutzern zurück, die es bereits besitzen. Nutzen Sie diese Option, wenn das Cybersicherheitsrisiko für die Nutzerinnen und Nutzer erheblich ist und eine Korrektur oder eine Marktrücknahme allein nicht ausreichen.

Die Wahl ist verhältnismäßig zum Risiko, keine starre Reihenfolge. Eine patchbare Schwachstelle mit funktionierender Korrektur bedeutet meist *In Konformität bringen*. Ein Produkt, das im Feld nicht sicher korrigiert werden kann, bedeutet meist *Vom Markt nehmen* und, sofern es bei erheblichem Risiko aktiv genutzt wird, *Rückrufen*.

Was Sie zusätzlich tun müssen

- **Melden Sie über die Kette nach Artikel 14**, wenn die Nichtkonformität eine aktiv ausgenutzte Schwachstelle oder ein schwerwiegender Sicherheitsvorfall ist. Die Meldefristen stehen oben.
- **Informieren Sie Nutzerinnen und Nutzer** über die Nichtkonformität und über Korrekturmaßnahmen, die sie selbst anwenden können. Siehe *Ihre Nutzerinnen und Nutzer informieren* oben für die Verhältnismäßigkeitsregeln.
- **Kooperieren** Sie mit jeder begründeten Anfrage einer Marktüberwachungsbehörde, einschließlich der Bereitstellung der technischen Dokumentation in einer Sprache, die die Behörde lesen kann.
- **Sichern Sie Nachweise.** Bewahren Sie die Aufzeichnungen, die zeigen, was Sie gefunden haben, wann Sie es gefunden haben, was Sie unternommen haben und wie Sie mit Nutzerinnen, Nutzern und Behörden kommuniziert haben. Die technische Dokumentation und die EU-Konformitätserklärung müssen mindestens 10 Jahre nach dem Inverkehrbringen oder für den gesamten Supportzeitraum verfügbar bleiben, je nachdem, welcher Zeitraum länger ist.

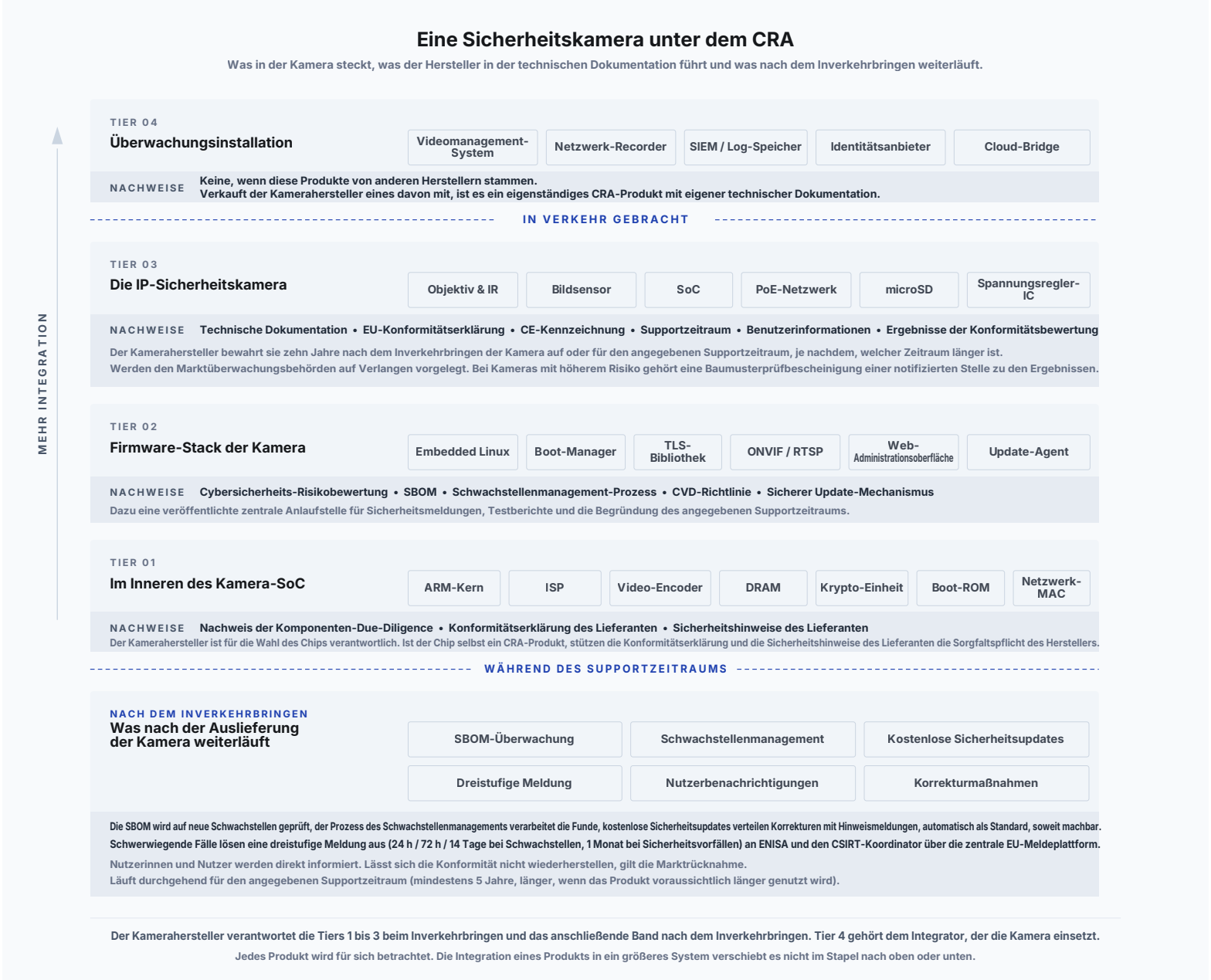
Anforderungen an die Produktdokumentation

Die Dokumentation muss **mindestens 10 Jahre** nach dem Inverkehrbringen des Produkts oder für den **gesamten Supportzeitraum** aufbewahrt werden, je nachdem, welcher Zeitraum länger ist. Auf Übersichtsebene benötigt die technische Dokumentation acht Nachweisfamilien:

1. Allgemeine Produktbeschreibung
2. Angaben zu Entwurf, Entwicklung und Produktion (einschließlich SBOM)
3. Cybersicherheits-Risikobewertung
4. Festlegung des Supportzeitraums
5. Angewandte harmonisierte Normen und Spezifikationen
6. Prüfberichte
7. EU-Konformitätserklärung
8. Vollständige SBOM (auf Verlangen von Marktüberwachungsbehörden)

Checkliste für den Konformitätsbewertungsweg

Nutzen Sie die Klassifizierungstabelle oben, um den Weg zu bestimmen. Halten Sie die Routenentscheidung anschließend in der technischen Dokumentation fest, zusammen mit den Normen, Spezifikationen, dem Zertifizierungsschema oder dem Nachweis der notifizierten Stelle, mit dem sie begründet wird.



Ein konkretes Beispiel. Dieselbe gestufte Struktur gilt für jedes Produkt mit digitalen Elementen, nicht nur für Sicherheitskameras.

Die Anforderungen an die Produktsicherheit

a. Keine bekannten ausnutzbaren Schwachstellen zum Zeitpunkt des Inverkehrbringens

Liefern Sie kein Produkt mit öffentlich bekannten ausnutzbaren Schwachstellen aus, die unbehandelt bleiben. Eine bekannte Schwachstelle kann aus einer öffentlichen Datenbank, einem Lieferantenhinweis, einer Kundenmeldung oder Ihrem eigenen internen Tracker stammen.

Um diese Anforderung zu erfüllen:

- Prüfen Sie vor jeder Veröffentlichung Schwachstellendatenbanken, einschließlich Common Vulnerabilities and Exposures, CVE
- Nutzen Sie statische und dynamische Anwendungssicherheitstests (SAST/DAST) in Ihrer Build-Pipeline
- Führen Sie Dependency-Scanning für alle Drittanbieter- und Open-Source-Komponenten durch
- Dokumentieren Sie Ihre Risikoakzeptanz oder Minderungsentscheidung für jedes identifizierte Problem

b. Sichere Standardkonfiguration

Das Produkt sollte im Auslieferungszustand sicher nutzbar sein. Deaktivieren Sie unnötige Dienste, vermeiden Sie schwache Standardzugangsdaten und halten Sie unsichere Inbetriebnahmemodi kurz und kontrolliert. Die Pflicht zur sicheren Standardkonfiguration kann für maßgeschneiderte Produkte, die gewerblichen Nutzern auf Grundlage einer schriftlichen Vereinbarung bereitgestellt werden, abweichend geregelt werden, sofern die Möglichkeit erhalten bleibt, das Produkt in seinen ursprünglichen sicheren Zustand zurückzusetzen.

Um diese Anforderung zu erfüllen:

- Deaktivieren Sie Fernzugriffsports und Debug-Schnittstellen in Standard-Builds
- Erzwingen Sie starke Standard-Authentifizierungsmechanismen
- Beschränken Sie administrative Funktionen auf befugte Nutzer
- Setzen Sie einen sicheren Werksreset um, der alle Einstellungen und die Firmware auf einen bekannten sicheren Zustand zurücksetzt und Nutzerdaten entfernt

c. Sicherheitsupdates, einschließlich automatischer Updates mit Opt-out

Das Produkt benötigt einen Patch-Mechanismus, der Sicherheitsprobleme nach der Bereitstellung bearbeiten kann. Wenn automatische Updates angemessen sind, aktivieren Sie sie standardmäßig und geben Sie Nutzern eine klare Möglichkeit, sie aufzuschieben oder abzulehnen.

Um diese Anforderung zu erfüllen:

- Setzen Sie kryptografische Signaturen und Integritätsprüfungen für Update-Pakete um
- Sorgen Sie für Rollback-Schutz und Protokollierung von Update-Ereignissen
- Bauen Sie Benachrichtigungssysteme auf, die Nutzer auf ausstehende Updates hinweisen
- Erlauben Sie Nutzern, automatische Updates über eine klare Konfigurationsoberfläche aufzuschieben oder zu deaktivieren

d. Schutz vor unbefugtem Zugriff

Zugriffskontrollen müssen lokale und entfernte Schnittstellen schützen. Ziel ist, unbefugte Nutzer von Funktionen, Daten, Konfiguration und Verwaltungsoberflächen fernzuhalten.

Um diese Anforderung zu erfüllen:

- Erzwingen Sie Richtlinien für Passwortkomplexität und starke Standardzugangsdaten
- Setzen Sie Multi-Faktor-Authentifizierung (MFA) ein, wo sie angemessen ist
- Nutzen Sie rollenbasierte Zugriffskontrolle (RBAC) und Session-Timeouts
- Protokollieren Sie erfolglose Zugriffsversuche, nutzen Sie Anomalieerkennung, um unbefugte Aktivitäten zu markieren, und stellen Sie diese Ereignisse zur Überprüfung und Meldung bereit

e. Vertraulichkeit gespeicherter, übertragener und verarbeiteter Daten

Sensible Daten brauchen Schutz im Ruhezustand, bei der Übertragung und während der Verarbeitung.

Um diese Anforderung zu erfüllen:

- Nutzen Sie standardisierte Verschlüsselungsalgorithmen, etwa AES-256 für ruhende Daten und TLS für Daten bei der Übertragung
- Wenden Sie sichere Verfahren für das Schlüsselmanagement an
- Trennen Sie vertrauliche Daten von nicht kritischen Systemkomponenten
- Führen Sie Audit-Logs für alle Datenzugriffe

f. Integrität von Daten, Firmware und Konfiguration

Diese Anforderung betrifft das System selbst, also Firmware, Software und Konfigurationsdateien, sowie die Daten, die es verarbeitet, etwa Messwerte, Steuerbefehle und Nutzereingaben.

Um diese Anforderung zu erfüllen:

- Setzen Sie Secure Boot und signierte Firmware ein, damit nur vertrauenswürdiger Code ausgeführt wird
- Nutzen Sie Laufzeitverifikation, um Manipulationsversuche zu erkennen und zu melden
- Wenden Sie kryptografisches Hashing und digitale Signaturen an, um Datenintegrität zu schützen
- Bauen Sie Infrastruktur auf, die kryptografische Schlüssel über System- oder Organisationsgrenzen hinweg erzeugen, verteilen und verifizieren kann

g. Datenminimierung

Erheben und verarbeiten Sie nur die Daten, die für den vorgesehenen Zweck des Produkts notwendig sind. Das gilt für personenbezogene und technische Daten.

Um diese Anforderung zu erfüllen:

- Führen Sie Datenschutz-Folgenabschätzungen oder Data-Protection-by-Design-Prüfungen durch, um unnötige Datenflüsse zu identifizieren
- Entfernen Sie ungenutzte Telemetrie, Diagnose oder Hintergrunddatenerfassung oder machen Sie sie optional
- Setzen Sie konfigurierbare Datenerfassung um, damit erweiterte Erfassung je nach Kontext ein- oder ausgeschaltet werden kann

h. Verfügbarkeit und Resilienz, auch gegen Denial-of-Service-Angriffe

Bei Sicherheitsvorfällen oder Angriffen sollten zentrale Produktfunktionen verfügbar bleiben oder kontrolliert ausfallen.

Um diese Anforderung zu erfüllen:

- Setzen Sie Circuit Breaker, Retry-Logik, Fallback-Mechanismen und Watchdog-Timer um
- Wenden Sie Ressourcenlimits an, um Ressourcenerschöpfung zu verhindern
- Nutzen Sie Rate Limiting und Eingabevalidierung zum Schutz vor Denial-of-Service-Szenarien
- Wenden Sie netzwerkseitige Filter an, um Überlastungsversuche zu blockieren

i. Keine negativen Auswirkungen auf andere verbundene Geräte oder Netze

Das Produkt sollte andere Systeme in derselben Umgebung nicht stören. Es sollte berechenbar arbeiten und gemeinsame Ressourcen nicht übermäßig beanspruchen.

Um diese Anforderung zu erfüllen:

- Setzen Sie Traffic Shaping um und begrenzen Sie Broadcast- oder Multicast-Nutzung
- Stellen Sie die Einhaltung der Spezifikationen für Kommunikationsprotokolle sicher
- Nutzen Sie Selbstüberwachung, um störendes Verhalten wie Network Flooding oder Ressourcenerschöpfung zu erkennen und zu verhindern

j. Begrenzte Angriffsfläche, einschließlich externer Schnittstellen

Minimieren Sie Einstiegspunkte und exponierte Funktionen. Dazu gehören physische Ports, Funkschnittstellen, APIs, Debug-Dienste und unnötige Softwarekomponenten.

Um diese Anforderung zu erfüllen:

- Deaktivieren Sie ungenutzte Dienste, Ports und Schnittstellen in Produktions-Builds
- Härten Sie Systemstandards und begrenzen Sie Nutzerrechte
- Modularisieren Sie Softwarearchitekturen, um Komponenten voneinander zu isolieren
- Wenden Sie sichere Software-Designprinzipien an und führen Sie Threat Modeling durch, um unnötige Exponierung zu erkennen und zu entfernen

k. Verringerte Auswirkungen von Sicherheitsvorfällen durch Exploitation-Mitigation

Gehen Sie davon aus, dass manche Angriffe erfolgreich sein werden. Das Produktdesign sollte begrenzen, wie weit sich Schaden ausbreiten kann.

Um diese Anforderung zu erfüllen:

- Trennen Sie Systemkomponenten und führen Sie sie in isolierten Umgebungen aus, etwa durch Sandboxing oder Containerisierung
- Erzwingen Sie Rechte-Trennung, damit kritische Funktionen nur mit den mindestens erforderlichen Berechtigungen laufen
- Gestalten Sie das System so, dass die Kompromittierung einer Komponente einem Angreifer nicht die Kontrolle über das gesamte System gibt

l. Protokollierung sicherheitsrelevanter Aktivitäten mit Opt-out für Nutzer

Zeichnen Sie sicherheitsrelevante Aktivitäten auf, etwa Zugriffsversuche und Datenänderungen, damit sie überwacht und geprüft werden können. Nutzer benötigen einen Opt-out-Mechanismus, wenn der CRA ihn verlangt.

Um diese Anforderung zu erfüllen:

- Setzen Sie strukturierte Protokollierung um, etwa JSON-Logs mit Zeitstempeln
- Stellen Sie lokale Log-Speicherung mit Log-Rotation und Optionen für Remote-Log-Streaming bereit
- Überwachen Sie Ereignisse wie Anmeldeversuche, Konfigurationsänderungen und Softwareupdates auf Anomalien
- Stellen Sie einen klaren nutzerseitigen Mechanismus bereit, um Protokollierung zu deaktivieren, soweit dies erlaubt ist

m. Sichere und dauerhafte Datenlöschung und Portabilität

Nutzer benötigen einen praktikablen Weg, Daten und Einstellungen dauerhaft zu entfernen. Wenn Daten auf ein anderes Produkt oder System übertragen werden können, muss die Übertragung sicher sein.

Um diese Anforderung zu erfüllen:

- Setzen Sie eine sichere Löschfunktion um, die Speicherbereiche überschreibt oder Schlüssel kryptografisch löscht
- Nutzen Sie authentifizierte und verschlüsselte Kanäle für Datenportabilität, um Offenlegung während der Übertragung zu verhindern

Die Anforderungen an das Schwachstellenmanagement

1. Schwachstellen identifizieren und dokumentieren

Sie müssen wissen, welche Softwarekomponenten im Produkt enthalten sind und welche bekannten Schwachstellen sie betreffen. Eine Software Bill of Materials (SBOM) liefert dieses maschinenlesbare Inventar.

Um diese Anforderung zu erfüllen:

- Integrieren Sie die SBOM-Erstellung direkt in Ihre CI/CD-Pipeline, damit jeder Build ein aktuelles Komponenteninventar erzeugt
- Nutzen Sie etablierte Formate wie CycloneDX, SPDX oder SWID für Interoperabilität
- Führen Sie automatisierte Schwachstellenscans gegen CVE-Listen und Datenbanken wie CISA KEV und ENISA EUVD durch
- Pflegen Sie die SBOM während des gesamten Supportzeitraums als Teil Ihrer technischen Dokumentation und stellen Sie sie Marktüberwachungsbehörden auf Anfrage bereit

2. Risikomanagement und zeitnahe Sicherheitsupdates

Wenn Schwachstellen gefunden werden, beheben Sie sie schnell und liefern Sie Sicherheitsupdates aus. Trennen Sie Sicherheits-Patches nach Möglichkeit von Funktionsupdates, damit kritische Korrekturen zeitnah installiert werden können.

Um diese Anforderung zu erfüllen:

- Gestalten Sie Ihren Update-Mechanismus so, dass Sicherheitskorrekturen ohne vollständiges Systemupdate ausgerollt werden können
- Strukturieren Sie Software und Firmware so, dass kritische Komponenten unabhängig gepatcht werden können
- Liefern Sie Updates über sichere Kanäle mit Integritätsprüfungen aus
- Führen Sie Aufzeichnungen über Update-Aktivitäten, um Nachvollziehbarkeit zu stützen und Compliance nachzuweisen

3. Regelmäßige Sicherheitstests

Sicherheitstests sind keine einmalige Aufgabe. Testen Sie Produkte über den gesamten Lebenszyklus, wenn sich Bedrohungen, Abhängigkeiten und Produktverhalten ändern. Die Risikobewertung sollte Art und Häufigkeit der Tests steuern.

Um diese Anforderung zu erfüllen:

- Führen Sie Penetrationstests durch, um reale Angriffe zu simulieren
- Wenden Sie statische und dynamische Codeanalyse an, um Sicherheitsschwächen zu identifizieren
- Nutzen Sie Fuzz-Testing, um Fehler in der Eingabeverarbeitung offenzulegen
- Planen und dokumentieren Sie Sicherheits-Code-Reviews und Architektur-Reviews formell, besonders nach wesentlichen Design- oder Funktionsänderungen

4. Schwachstellen-Annahme, CVD-Richtlinie und Advisories

Deckt die Pflichten zur Annahme von Meldungen, zur koordinierten Offenlegung und zu Advisories (Punkte 4, 5 und 6 der obigen Übersicht) ab, die in der Praxis als ein gemeinsamer Workflow laufen.

Der CRA benennt drei separate Anforderungen dafür, wie Sie rund um Schwachstellen kommunizieren: einen Weg, über den Personen Probleme melden können, eine Richtlinie für koordinierte Offenlegung und ein Advisory, wenn Sie eine Korrektur ausliefern. So sehen die einzelnen Pflichten aus.

Annahme

Geben Sie Meldenden einen klaren, niedrigschwelligen Zugang. Veröffentlichen Sie eine sichtbare Kontaktmethode für Schwachstellenmeldungen (eigene E-Mail-Adresse oder Webformular). Unterstützen Sie sichere Kommunikation, etwa durch Veröffentlichung eines PGP-Schlüssels. Die Pflicht erfasst Meldungen zu Ihrem eigenen Produkt und zu den darin enthaltenen Drittanbieterkomponenten.

Triage

Bestätigen Sie jede Meldung, erfassen Sie sie in einem Tracking-System, weisen Sie sie zur Prüfung zu und lösen Sie sie innerhalb definierter Fristen. Senden Sie Bestätigungen und Statusupdates an die meldende Seite zurück. Sitzt das Problem in einer Drittanbieterkomponente, leiten Sie es parallel zu Ihrer eigenen Behebung an die Upstream-Maintainer weiter.

Richtlinie für koordinierte Offenlegung von Schwachstellen

Veröffentlichen Sie eine CVD-Richtlinie, die Erwartungen für Meldende und Partner setzt: Kontaktmethode, erwartete Reaktionszeiten, wozu Sie sich verpflichten, was Sie von ihnen erwarten. Koordinieren Sie die Offenlegung so, dass Nutzerinnen und Nutzer geschützt werden und der Beitrag der meldenden Seite anerkannt bleibt.

Advisories bei Behebung

Sobald eine Korrektur verfügbar ist, veröffentlichen Sie ein Advisory zum gelösten Problem. Nennen Sie die CVE-Kennung, die betroffenen Produktversionen, eine standardisierte Schweregradbewertung (etwa CVSS) und klare, zugängliche Informationen zu dem, was Nutzerinnen und Nutzer tun sollten. Formulieren Sie in einer Sprache, die sowohl technische Administratorinnen und Administratoren als auch nicht technische Nutzerinnen und Nutzer verstehen.

Verzögerte öffentliche Offenlegung

Sie dürfen die öffentliche Offenlegung nur aus einem hinreichend begründeten Anlass verzögern, wenn die Cybersicherheitsrisiken einer sofortigen Offenlegung die Vorteile überwiegen, und nur bis Nutzerinnen und Nutzer die Möglichkeit hatten, die Korrektur anzuwenden. Dokumentieren Sie die Begründung.

5. Sichere Mechanismen zur Verteilung von Updates

Der Update-Mechanismus muss zuverlässig und manipulationsresistent sein. Automatische Updates verkürzen, soweit technisch machbar, die Zeit, in der Nutzer exponiert bleiben.

Um diese Anforderung zu erfüllen:

- Übertragen Sie Updates über sichere Kanäle und verifizieren Sie sie durch digitale Signaturen
- Wenden Sie Updates so an, dass unvollständige oder beschädigte Installationen verhindert werden
- Nutzen Sie differenzielle oder modulare Updates, um Störungen zu reduzieren und Korrekturen schneller auf Systeme zu bringen
- Führen Sie Update-Logs, damit Nutzer oder Administratoren den Update-Status verifizieren können

6. Kostenlose Sicherheitsupdates mit Hinweismeldungen

Liefern Sie Sicherheitsupdates zeitnah und ohne zusätzliche Kosten aus, außer wenn für maßgeschneiderte Geschäftsprodukte eine gesonderte Vereinbarung besteht. Jedes Update benötigt eine klare Hinweismeldung, die Nutzerinnen und Nutzern sagt, was sich geändert hat und was zu tun ist.

Um diese Anforderung zu erfüllen:

- Betreiben Sie ein Verteilungssystem, das Nutzer direkt benachrichtigen oder Updates je nach Produktkontext automatisch anwenden kann
- Schreiben Sie Hinweismeldungen in einer Sprache, die technische und nicht technische Nutzer verstehen
- Nehmen Sie Schweregradinformationen in Hinweismeldungen auf, wenn sie relevant sind
- Sagen Sie Nutzerinnen und Nutzern, welche Handlung zu ergreifen ist, etwa das Anwenden des Updates, eine Konfigurationsänderung oder die Beobachtung möglicher Anzeichen einer Kompromittierung
- Verteilen Sie Sicherheitsupdates ohne Verzögerung, sobald sie verfügbar sind, damit Nutzerinnen und Nutzer nicht exponiert bleiben, während die Korrektur bereits existiert
- Veröffentlichen Sie Advisories über einen vom Hersteller kontrollierten Kanal und verlinken Sie sie von der Supportseite des Produkts aus

Die Pflichten zur unentgeltlichen und unverzüglichen Auslieferung laufen für die Dauer des erklärten Supportzeitraums. Die Ausnahme für maßgeschneiderte Produkte ändert nur die kommerzielle Grundlage; Hinweismeldungen bleiben verpflichtend.

Was in die technische Dokumentation gehört

Technische Dokumentation

Die technische Dokumentation ist der zentrale Nachweis für CRA-Compliance. Sie muss die gestalterischen, technischen und prozessualen Maßnahmen abdecken, mit denen die grundlegenden Cybersicherheitsanforderungen erfüllt werden. Sie muss **vor dem Inverkehrbringen** vorliegen und während des gesamten **Supportzeitraums** aktuell bleiben.

Nachweise der technischen Dokumentation im Engineering-Ablauf

Schritt 1	**Abgrenzen und klassifizieren**	Produktzweck, vorgesehene Verwendung, Inverkehrbringen, Produktklasse, Normenroute.
Schritt 2	**Architektur und Risiko**	Architektur, Datenverbindungen, Nutzungsbedingungen, Risikobewertung, Minderungen.
Schritt 3	**Komponenten und SBOM**	Maschinenlesbare SBOM, Drittanbieterkomponenten, Lieferantenangaben, Schwachstellenverfolgung.
Schritt 4	**Build, Test, Update**	Sichere Standardwerte, Härtung, Testberichte, sicherer Update-Mechanismus, Hinweise an Nutzer.
Schritt 5	**Freigabe und Support**	Benutzerinformationen, EU-Erklärung, CE-Nachweise, Supportbegründung, Update-Aufzeichnungen.

Die technische Dokumentation umfasst acht erforderliche Bestandteile. Zusammen erklären sie, **was das Produkt ist**, **wie es entwickelt und getestet wurde**, **welche Risiken berücksichtigt wurden**, **welche Normen angewandt wurden** und **wie es unterstützt wird**, sobald es am Markt ist. Sie müssen die rechtlichen Überschriften nicht kopieren, doch jedes Thema muss abgedeckt sein.

Nr.	Bestandteil	Was enthalten sein muss
1	Allgemeine Produktbeschreibung	Bestimmungsgemäßer Zweck und Funktionen, relevante Softwareversionen, Fotos oder Abbildungen (bei Hardware), Benutzerinformationen und Anleitungen
2	Angaben zu Entwurf, Entwicklung und Produktion	Architekturbeschreibung (Komponenten und Interaktionen), Software Bill of Materials (SBOM), Prozesse für das Schwachstellenmanagement (CVD-Richtlinie, Kontaktstelle, sichere Update-Mechanismen), Produktions- und Überwachungsprozesse einschließlich Validierung
3	Cybersicherheits-Risikobewertung	Dokumentierte Analyse der Produktrisiken, Erläuterung, wie jede grundlegende Cybersicherheitsanforderung auf das Produkt anwendbar ist, Minderung identifizierter Risiken
4	Festlegung des Supportzeitraums	Dokumentation der Faktoren, die zur Festlegung des Supportzeitraums genutzt wurden, etwa Nutzererwartungen, vergleichbare Produkte und rechtliche Orientierung
5	Angewandte harmonisierte Normen und Spezifikationen	Liste angewandter harmonisierter Normen, gemeinsamer Spezifikationen oder EU-Zertifizierungssysteme; Angabe, ob vollständig oder teilweise angewandt; alternative Lösungen, wenn Normen nicht angewandt werden
6	Prüfberichte	Konformitätsnachweise für das Produkt und die Prozesse zum Schwachstellenmanagement
7	EU-Konformitätserklärung	Kopie der Erklärung, die die technische Dokumentation mit den Pflichten zur CE-Kennzeichnung verknüpft
8	Vollständige SBOM (auf Anfrage)	Marktüberwachungsbehörden können die vollständige SBOM verlangen, um Compliance zu verifizieren

Eine einzige konsolidierte technische Dokumentation kann den CRA und andere anwendbare EU-Rechtsvorschriften abdecken, etwa die Funkanlagenrichtlinie oder die ESPR, sofern alle anwendbaren Pflichten enthalten sind.

EU-Konformitätserklärung

Die EU-Konformitätserklärung ist die formelle Erklärung des Herstellers, dass das Produkt die anwendbaren Cybersicherheitsanforderungen des CRA erfüllt. Jede Erklärung muss enthalten:

- Produktname, Typ und eindeutige Kennungen
- Name und Anschrift des Herstellers oder seines Bevollmächtigten
- Erklärung der alleinigen Verantwortung des Anbieters
- Produktbeschreibung, die Rückverfolgbarkeit sicherstellt, optional mit Bild
- Ausdrückliche Erklärung der Konformität mit einschlägigem Unionsrecht
- Verweise auf angewandte harmonisierte Normen, Spezifikationen oder Zertifizierungen
- Angaben zu beteiligten notifizierten Stellen (Name, Nummer, Verfahren, Zertifikatsnummer)
- Unterschriftsblock: Ort, Datum, Name, Funktion und Unterschrift der unterzeichnenden Person

Nach Unterzeichnung ist die Erklärung rechtsverbindlich und bestätigt die volle Verantwortung des Herstellers für Cybersicherheits-Compliance.

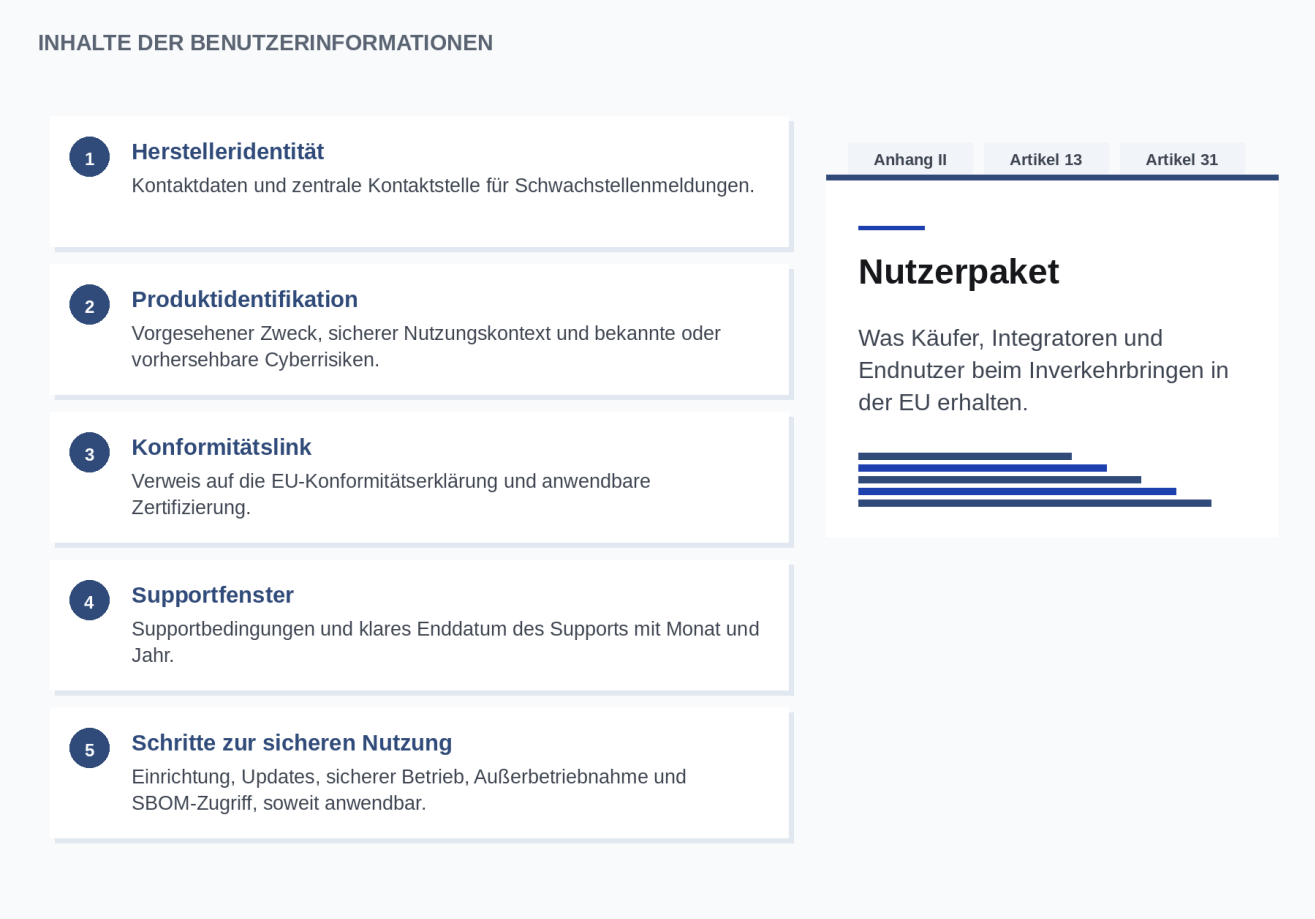
Eine vereinfachte Erklärung ist für Verpackungen oder Handbücher zulässig, in der Form: „Hiermit erklärt [Hersteller], dass das Produkt [Typ/Bezeichnung] der Verordnung (EU) 2024/2847 entspricht. Der vollständige Text der EU-Konformitätserklärung ist unter folgender Internetadresse verfügbar: [Internetadresse]." Diese vereinfachte Form erhält Transparenz und reduziert Papieraufwand. Sie ist besonders nützlich für kleine Hersteller oder Portfolios mit mehreren Produkten.

Benutzerinformationen und Anleitungen

Benutzerinformationen und Anleitungen sind eine Voraussetzung für rechtmäßiges Inverkehrbringen. Hersteller müssen Anleitungen mindestens **10 Jahre** oder während des gesamten **Supportzeitraums** verfügbar halten. Einführer und Händler müssen prüfen, ob die Anleitungen vorhanden, aktuell und in der richtigen EU-Sprache bereitgestellt sind, bevor sie das Produkt in Verkehr bringen oder liefern.

Die Benutzeranleitungen müssen enthalten:

- Identität und Kontaktdaten des Herstellers
- Eine zentrale Kontaktstelle für Schwachstellenmeldungen
- Produktidentifikation, vorgesehener Zweck und sicherer Nutzungskontext
- Bekannte oder vorhersehbare Cyberrisiken
- Link zur EU-Konformitätserklärung
- Supportbedingungen und klares Enddatum des Supports
- Schrittweise Sicherheitsanleitungen für Einrichtung, Updates, sichere Nutzung, Außerbetriebnahme und, soweit anwendbar, Integration und SBOM-Zugriff



Der richtige Weg der Konformitätsbewertung

Modul A: Selbstbewertung

Modul A (interne Fertigungskontrolle) erlaubt Ihnen, selbst zu bescheinigen, dass Ihr Produkt die grundlegenden Cybersicherheitsanforderungen erfüllt. Sie übernehmen dabei die volle Verantwortung für Entwurf und Produktion. Dieser Weg steht Herstellern von Standardprodukten, also nicht klassifizierten Produkten, offen. Für wichtige Produkte der Klasse I steht er nur offen, wenn die einschlägigen harmonisierten Normen, gemeinsamen Spezifikationen oder europäischen Cybersicherheitszertifizierungssysteme verfügbar sind und wie vom CRA verlangt angewandt werden.

Unter Modul A müssen Sie:

- Umfassende technische Dokumentation erstellen
- Entwurf, Produktionsprozesse, Cybersicherheitsmechanismen und Verfahren zum Schwachstellenmanagement des Produkts detailliert beschreiben
- Die laufende Verantwortung für fortgesetzte Compliance während des Produktlebenszyklus behalten
- Einen Plan für Sicherheitsupdates und Schwachstellenmanagement während der Betriebsdauer des Produkts umsetzen
- Aufzeichnungen mindestens 10 Jahre verfügbar halten

Modul B und Modul C: produktbezogene Bewertung

Modul B und Modul C gelten, wenn eine Drittprüfung eines bestimmten Produkttyps erforderlich ist. Sie gelten für wichtige Produkte der Klasse I, wenn der Hersteller einschlägige harmonisierte Normen, gemeinsame Spezifikationen oder Zertifizierungssysteme nicht, nur teilweise oder nicht anwendbar nutzen kann. Für wichtige Produkte der Klasse II muss der Hersteller Modul B+C, Modul H oder ein anwendbares europäisches Cybersicherheitszertifizierungssystem mindestens auf Vertrauenswürdigkeitsstufe „substanziell" nutzen.

Modul B (EU-Baumusterprüfung): Eine notifizierte Stelle prüft ein repräsentatives Produktmuster und die zugehörige technische Dokumentation. Sie verifiziert die Erfüllung aller grundlegenden Cybersicherheitsanforderungen und stellt eine EU-Baumusterprüfbescheinigung aus, wenn das Produktdesign die CRA-Kriterien erfüllt.

Modul C (Konformität mit der Bauart, Produktionskontrolle): Der Hersteller stellt sicher, dass alle Produktionseinheiten dem nach Modul B genehmigten Baumuster entsprechen. Der Hersteller bringt die CE-Kennzeichnung an, stellt die EU-Konformitätserklärung aus und hält Aufzeichnungen mindestens 10 Jahre verfügbar. Zusammen stellen Modul B und Modul C sicher, dass ein bestimmtes Produktmodell technisch konform ist und jede Produktionscharge mit dem genehmigten Design übereinstimmt.

Modul H: prozessbezogene Bewertung (umfassende Qualitätssicherung)

Modul H (umfassende Qualitätssicherung) konzentriert sich auf das gesamte interne Qualitätssystem des Herstellers und nicht auf einzelne Produkttests. Es steht für wichtige Produkte der Klassen I und II zur Verfügung. Kritische Produkte nutzen den Zertifizierungsweg, wenn die einschlägigen Bedingungen erfüllt sind. Wenn diese Bedingungen nicht erfüllt sind, nutzen sie dieselben Wege wie wichtige Produkte der Klasse II.

Unter Modul H müssen Sie:

- Ein Qualitätssystem einrichten und aufrechterhalten, das Entwurf, Entwicklung, Produktion, Tests und Schwachstellenmanagement für die gesamte Produktkategorie abdeckt
- Das Qualitätssystem einer notifizierten Stelle zur Bewertung und Genehmigung vorlegen
- Laufende Überwachung durch die notifizierte Stelle akzeptieren, einschließlich Audits, Inspektionen und Prozessreviews zur Verifizierung fortlaufender Compliance

Nach Genehmigung dürfen Sie Konformitätserklärungen für alle Produkte ausstellen, die unter diesem Qualitätssystem hergestellt werden, ohne die Prüfung durch die notifizierte Stelle für jeden einzelnen Produkttyp zu wiederholen.

Der wichtigste Unterschied zwischen den Wegen:

- Modul B+C: Fokus auf dem Produkt. Ein repräsentativer Produkttyp wird geprüft und zertifiziert.
- Modul H: Fokus auf dem Prozess. Das gesamte Entwurfs- und Produktionssystem des Herstellers wird zertifiziert und überwacht.

WEGE DER KONFORMITÄTSBEWERTUNG

A

MODUL

Selbstbewertung

Standardprodukte und wichtige Klasse I, wenn harmonisierte Normen, gemeinsame Spezifikationen oder Zertifizierungssysteme vollständig angewandt werden. Der Hersteller übernimmt die volle Verantwortung für Entwurf und Produktion.

B+C

MODUL

Typ und Produktion

Erforderlich für wichtige Klasse I ohne anwendbare Normen und als Teil des Wegs für wichtige Klasse II. Eine notifizierte Stelle prüft einen repräsentativen Typ; der Hersteller stellt sicher, dass jede Produktionseinheit konform ist.

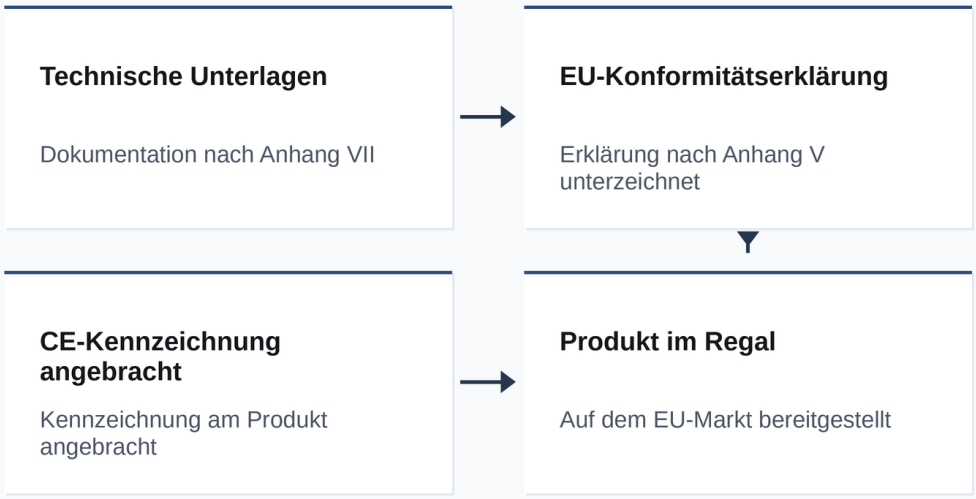
H

MODUL

Umfassende Qualitätssicherung

Verfügbar für wichtige Klasse I und II. Die notifizierte Stelle genehmigt und auditiert das Entwurfs-, Entwicklungs-, Produktions-, Test- und Schwachstellenmanagementsystem des Herstellers durchgängig.

Ablauf zum Inverkehrbringen



Der CRA im breiteren EU-Regulierungsumfeld

Der CRA steht nicht allein. Die praktische Frage für einen Hersteller lautet: Wo spart meine CRA-Arbeit Aufwand unter einem anderen EU-Regime, und wo bestehen weiterhin separate Pflichten parallel?

Wo Ihre CRA-Arbeit weiterverwendet werden kann

- **Hochrisiko-KI-Systeme (AI Act, Verordnung 2024/1689).** Ist Ihr Produkt ein Hochrisiko-KI-System im Anwendungsbereich des CRA, gilt die Erfüllung der grundlegenden Cybersicherheitsanforderungen des CRA insoweit als Erfüllung der Cybersicherheitsanforderungen des AI Act, als sie von Ihrer EU-Konformitätserklärung abgedeckt sind. Das Konformitätsbewertungsverfahren läuft in der Regel über das Regime des AI Act, mit einer Ausnahme für wichtige und kritische CRA-Produkte. Die CRA-Cybersicherheits-Risikobewertung muss KI-spezifische Risiken wie Datenvergiftung und adversariale Angriffe berücksichtigen.
- **Konsolidierte Risikobewertung mit anderem Unionsrecht.** Der CRA lässt ausdrücklich zu, dass die Cybersicherheits-Risikobewertung Teil einer umfassenderen Risikobewertung wird, die ein anderer Rechtsakt der Union verlangt, wenn das Produkt unter beide Regime fällt. Ein Bewertungsartefakt, zwei regulatorische Nutzungen.
- **Eine technische Dokumentation über mehrere Regime.** Wie im Abschnitt zur technischen Dokumentation bereits erwähnt, kann eine einzige konsolidierte technische Dokumentation den CRA zusammen mit anderem anwendbaren Unionsrecht abdecken, solange die Pflichten jedes Regimes adressiert sind. Nützlich, wenn dasselbe Produkt bereits Dokumentation unter der Funkanlagenrichtlinie, der ESPR oder anderem Produktrecht benötigt.
- **Gemeinsame Definitionen von Wiederaufarbeitung, Wartung und Reparatur.** Der CRA übernimmt diese Definitionen aus der ESPR. Wenn Sie analysieren, ob ein Serviceeingriff als wesentliche Änderung zählt, sind die ESPR-Definitionen die Referenz, nicht ein CRA-eigener Begriff.

Wo separate Pflichten bestehen bleiben

- **AI Act, alles Übrige.** Cybersicherheit ist nur ein Ausschnitt des AI Act. Risikoklassifizierung, Transparenz, Daten-Governance, menschliche Aufsicht, Überwachung des KI-Verhaltens nach dem Inverkehrbringen und der Rest sind Pflichten des AI Act, die der CRA nicht adressiert. CRA-konforme Cybersicherheit ist keine Vermutung der Konformität mit dem AI Act insgesamt.
- **ESPR-Inhalte und digitaler Produktpass.** ESPR-Anforderungen zu Energieeffizienz, Langlebigkeit, Reparierbarkeitsbewertung und die Nachhaltigkeitsinhalte des digitalen Produktpasses liegen nicht im CRA-Anwendungsbereich. Die CRA-Nachweiskette kann neben der ESPR-Arbeit stehen, ersetzt sie aber nicht.
- **Data Act, Datenzugangsrechte bei IoT.** Der Data Act gibt Nutzerinnen und Nutzern vertragliche Rechte auf Zugang zu, Weitergabe und Übertragung der Daten, die ihre vernetzten Produkte erzeugen. Der CRA deckt die Sicherheit dieser Daten ab; er legt das Zugangsrechte-Regime nicht fest. Andere Pflicht, andere Nachweise.
- **Produkthaftung für fehlerhafte Produkte.** Die Produkthaftungsrichtlinie (2024/2853) belässt die verschuldensunabhängige Haftung beim Hersteller. Fehlende Sicherheitsupdates nach dem Inverkehrbringen können den haftungsauslösenden Mangel bilden. Verträge, Versicherungen und Vorfall-Playbooks sollten dieses Risiko unabhängig von der CRA-Konformität abdecken.

Wie CRA Evidence hilft

CRA Evidence überführt Pflichten aus dem EU Cyber Resilience Act in verifizierbare Produktnachweise und verbindet eine Compliance-Plattform mit technischer Beratung.

Plattform

Ein zentraler Ort für die Nachweise hinter der CRA-Bereitschaft:

- **SBOM- und Komponentenbestand:** CycloneDX-, SPDX- und HBOM-Nachweise für Produktversionen und Releases
- **CI/CD-Nachweisautomatisierung:** CLI- und API-Workflows für Scans, SBOM-Uploads, Release-Gates und Audit-Aufzeichnungen
- **Signierte SBOM und Herkunft:** versionierte Nachweise, Lieferantenbestätigungen und Due-Diligence-Unterlagen
- **Schwachstellenbetrieb:** CISA KEV, EPSS, VEX, Überwachung, Triage und Meldeworkflows
- **Technische Dokumentation und CE-Nachweise:** EU-Erklärungsdaten, Aufbewahrungshistorie und QR-verknüpfte Produkt-Compliance-Pässe

Technische Beratung

Gezielte Unterstützung, um CRA-Pflichten in Engineering-Entscheidungen für Produkt, Architektur, Release-Prozess und Lieferantenmodell zu übersetzen.

- **Sprint zur technischen Bereitschaft:** Gap-Review zu den grundlegenden Cybersicherheitsanforderungen, Architektur-Empfehlungen und priorisierter Aktionsplan
- **CRA-Programmleitung:** Verantwortungsmodell, Pflichtenverfolgung, Nachweis-Meilensteine und Pflege der technischen Dokumentation
- **Behörden- und Incident-Response-Plan:** Meldeworkflows, Anfrage-Playbooks, Nutzerkommunikation und Vorbereitung von Nachweispaketen
- **Regulatorische Abstimmung:** CRA-Nachweise mit Data Act, ESPR, AI Act, RED und sektoralen Anforderungen verbinden
- **Technische Workshops:** Remote- oder Vor-Ort-Sitzungen mit Produkt, Engineering, Sicherheit, Compliance und Lieferanten

Werkzeugneutral: CRA Evidence integriert sich mit CycloneDX, SPDX, Grype, Trivy, CI/CD-Pipelines und Issue-Trackern.

Ein praktischer erster Schritt

Wählen Sie eine Produktfamilie. Ordnen Sie Verantwortliche, Scope-Entscheidung, SBOM, Schwachstellenworkflow, Lücken in der technischen Dokumentation und Release-Nachweise zu. So erhält das Team eine konkrete CRA-Basis, ohne Compliance zu einem separaten Projekt zu machen.

Erkunden Sie auf craevidence.com, was CRA Evidence für Ihr Produkt leistet. Preise und Pläne finden Sie unter craevidence.com/pricing.