CRA Cybersecurity

Leitfaden zur Einordnung und Umsetzung für Produkte mit digitalen Elementen

Einordnung, Anforderungen und konkrete Handlungsschritte

steinel

Cybersecurity für vernetzte Produkte

Cybersecurity ist eine der zentralen Herausforderungen in der Europäischen Union.

Die Anzahl und Vielfalt vernetzter Geräte wächst stetig und erhöht die Angriffsfläche für Cyberrisiken.

Gleichzeitig führen Cyberangriffe, Schwachstellen und fehlende Sicherheitsupdates zu erheblichen Risiken, sowohl für Unternehmen als auch für die Sicherheit und Stabilität von Infrastruktur und Gesellschaft.

Der Cyber Resilience Act (CRA) adressiert diese Entwicklung und schafft einen verbindlichen regulatorischen Rahmen für Produkte mit digitalen Elementen in der Europäischen Union.

Hersteller sind erstmals verpflichtet, Cybersicherheit über den gesamten Produktlebenszyklus hinweg systematisch sicherzustellen, von der Entwicklung über den Betrieb bis hin zur laufenden Pflege und Aktualisierung.

Der CRA verändert damit grundlegend, wie Produkte entwickelt, betrieben und in Verkehr gebracht werden. Unternehmen stehen vor der Aufgabe, ihre bestehenden Produkte, Prozesse und Verantwortlichkeiten entsprechend anzupassen.

Dieses Whitepaper bietet eine strukturierte Einordnung der zentralen Anforderungen und zeigt die relevanten Aspekte entlang des gesamten Prozesses auf.

Strukturierter Zugang zum Thema CRA

Die Anforderungen des CRA betreffen unterschiedliche Bereiche, von der Einordnung der Produkte bis zur Konformität.

Ein strukturierter Einstieg umfasst insbesondere:

- Produktklassifizierung
- Pflichten der Hersteller
- Meldepflichten
- Konformität und Nachweisführung
- Ableitung konkreter Massnahmen

Die folgenden Abschnitte greifen diese Themen einzeln auf.

Produktklassifizierung nach dem CRA

Der Cyber Resilience Act führt ein EU-weit harmonisiertes Klassifizierungssystem für Produkte mit digitalen Elementen ein.

Ziel ist es, Cybersicherheitsanforderungen risikobasiert und verhältnismässig zu gestalten.

Die vier Produktkategorien im Überblick:

Standardprodukte (Default)
(ca. 90% der Produkte)
z.B. Smart-Home-Geräte, IoT-Sensoren oder Consumer Software

Wichtige Produkte – Klasse I
z.B. Produkte mit erhöhtem Cybersicherheitsrisiko, z.B. Betriebssysteme, Browser, Router oder Passwortmanager

Wichtige Produkte – Klasse II
z.B. Firewalls oder Container-Runtime-Systeme

Kritische Produkte
z.B. Hardware-Sicherheitsmodule oder Smart-Meter-Gateways.

Je nach Kategorie ergeben sich unterschiedliche Anforderungen und Konformitätsverfahren.

Konformitätsbewertung:

Intern möglich bei Standard- & teilweise Klasse I Produkten – externe Prüfung (notifizierte Stelle) erforderlich für Klasse II & kritische Produkte.

→ Die richtige Klassifizierung ist der erste und entscheidende Schritt und beeinflusst direkt Aufwand, Kosten und Markteinführung.

steinel

Pflichten der Hersteller

Der CRA verpflichtet Hersteller, Cybersicherheit systematisch über den gesamten Produktlebenszyklus sicherzustellen.

Zentrale Pflichten:

- Security by Design & by Default bereits bei Entwicklung und Design
- verpflichtende Cybersicherheits-Risikobewertung
- aktives Schwachstellenmanagement
- Bereitstellung von Sicherheitsupdates
- Berücksichtigung von Dritt- und Open-Source-Komponenten
- Transparenz gegenüber Nutzern
- technische Dokumentation, Konformitätsbewertung und CE-Kennzeichnung

→ Cybersicherheit wird damit zur dauerhaften Herstellerverantwortung über den gesamten Lebenszyklus.

Meldepflichten im Überblick

Der CRA verpflichtet Hersteller, Sicherheitsprobleme aktiv und strukturiert zu melden.

Meldepflichtig sind:

- aktiv ausgenutzte Schwachstellen
- schwerwiegende Sicherheitsvorfälle, z.B. bei Datenverlust, Funktionsbeeinträchtigung oder Schadcode

Meldeverfahren:

Die Meldung erfolgt über die einheitliche EU-Meldeplattform an:

- das zuständige CSIRT und
- die ENISA

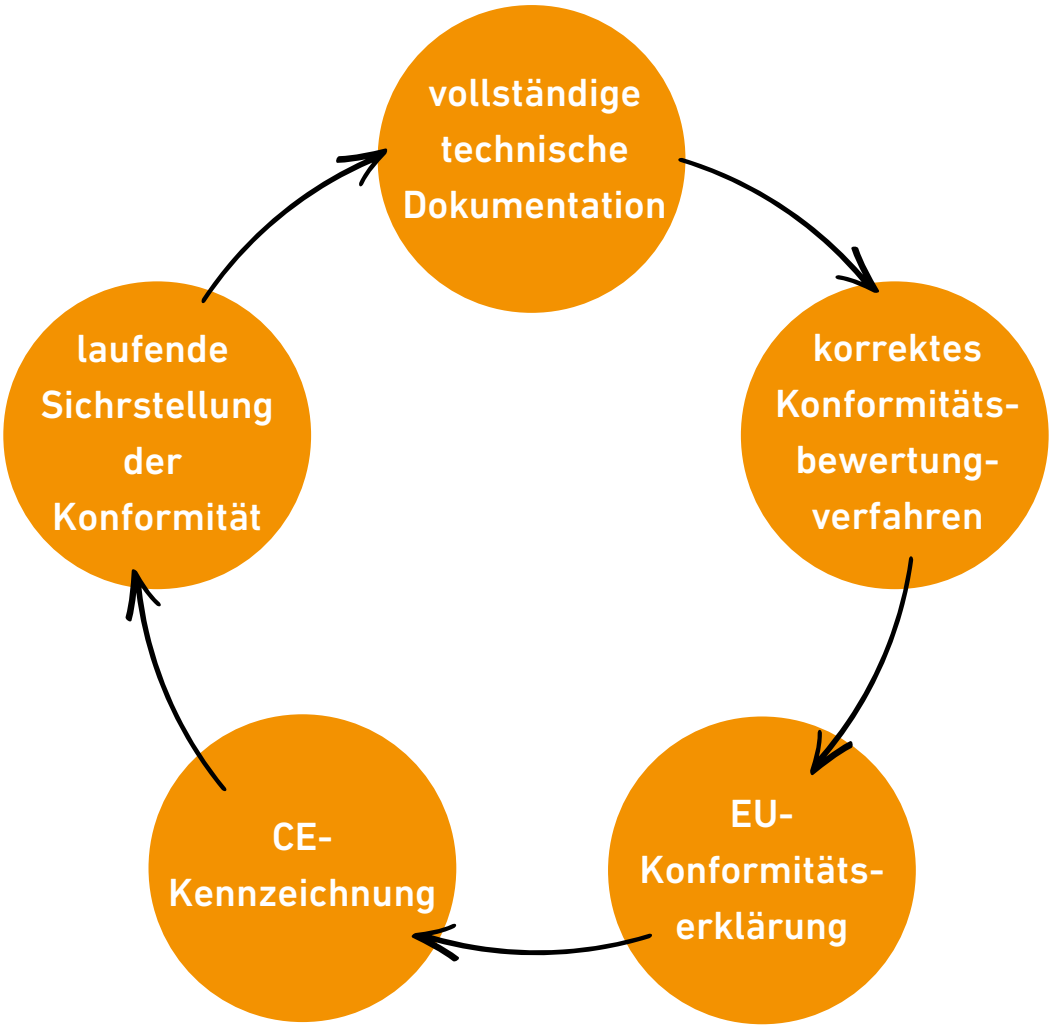
Zusätzlich besteht eine Informationspflicht gegenüber den Nutzern.

→ Sicherheitsvorfälle sind damit keine interne Angelegenheit mehr, sondern Teil regulatorischer Anforderungen.

Konformität von Produkten

Ein Produkt darf nur dann in der EU in Verkehr gebracht werden, wenn es nachweislich die Anforderungen des CRA erfüllt.

Dazu gehören:



Änderungen an Produkt, Prozessen oder Normen müssen laufend berücksichtigt werden.

Marktüberwachungsbehörden können bei Abweichungen Korrekturmassnahmen, Rückrufe oder Marktbeschränkungen anordnen.

Fazit & nächste Schritte

Der Cyber Resilience Act macht Cybersicherheit zur verbindlichen Herstellerpflicht.

Auch wenn die vollständige Anwendung erst ab 11. Dezember 2027 beginnt, entscheidet die Vorbereitung heute über die Zukunftsfähigkeit von Produkten und Prozessen.

Was Unternehmen jetzt tun sollten:

- Produkte und Portfolios auf CRA-Relevanz prüfen
- Produktklassifizierung durchführen
- Bevollmächtigter benennen wo nötig
- Sicherheits- und Entwicklungsprozesse bewerten und aufbauen
- Verantwortlichkeiten und Meldewege festlegen (bis September 2026)
- Dokumentation und Konformitätsnachweise frühzeitig aufbauen

→ Wer früh startet, reduziert Risiken, Kosten und regulatorischen Druck.

Empfohlene Vorgehensweise aufgrund der schrittweisen Einführung des CRA

JETZT

Durchführung einer Bestandsaufnahme: Welche Produkte fallen unter den CRA? Check durchführen und die Produkte in entsprechende Kategorien einordnen.

Interne Verantwortlichkeiten festlegen. Bevollmächtigte prüfen und gegebenenfalls benennen. Konformitätsstellen im Blick behalten.

bis Sept. 2026

Vorbereitung der Meldepflichten:
Interne Prozesse zur Erkennung und Meldung von Schwachstellen definieren und implementieren.

bis Dez. 2027

Technische Dokumentation erstellen. Konformitätserklärung ausarbeiten und CE-Kennzeichnung abschliessen. Konformitätsbewertung durchführen und eine Policy für das Schwachstellenmanagement umsetzen.

Laufend

ab Dez. 2027

Support-Zeitraum kontinuierlich überwachen (mindestens 5 Jahre). Sicherheitsupdates kostenfrei bereitstellen. Meldepflichten einhalten und Dokumentation stets aktuell halten.

steinel

Q&A

Für wen gilt der CRA?

Für Hersteller und Anbieter von Produkten mit digitalen Elementen in der EU.

Welche Produkte betrifft es?

Die Verordnung gilt für alle Produkte mit digitalen Elementen, die auf dem Markt bereitgestellt werden und deren Zweck oder vorhersehbare Verwendung eine direkte oder indirekte Datenverbindung zu anderen Geräten oder Netzwerken einschliesst.

Ein «Produkt mit digitalen Elementen» ist dabei ein Software- oder Hardwareprodukt inklusive zugehöriger Datenverarbeitungslösungen sowie auch einzelner Komponenten, die separat in Verkehr gebracht werden können.

Mein Gerät ist nicht am Internet – gilt der CRA trotzdem?

Ja, auch lokal betriebene Geräte können unter den CRA fallen.

Gibt es eine Meldepflicht?

Ja, für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle.

Q&A

Sind harmonisierte Normen schon vorhanden? (Stand Juni 2026)

Sie werden aktuell erarbeitet und sind wichtig für die praktische Umsetzung.

Muss ich schon etwas tun, solange Normen fehlen?

Ja. Wenn man auf die Veröffentlichung der Normen wartet, wird die Umsetzung sehr stressig. Viele Anforderungen sind bereits klar, Unternehmen können sich schon jetzt gezielt vorbereiten.

Muss ich bei meinem Produkt Informationen zu CRA-Anforderungen ergänzen?

Ja. Hersteller müssen relevante Informationen zur Cybersicherheit und zum sicheren Einsatz des Produkts bereitstellen. Dazu gehören insbesondere Hinweise zu Sicherheitsfunktionen, Updates und dem Umgang mit Schwachstellen, diese Informationen müssen für Kunden verständlich zugänglich sein.

Noch offene Fragen?

Oft bleiben individuelle Fragen offen, insbesondere bei der konkreten Einordnung von Produkten oder der Umsetzung der Anforderungen.

Genau hier unterstützen wir Sie.

Wir helfen Ihnen dabei:

- Ihre konkrete Ausgangssituation einzuordnen
- erste Handlungsfelder zu identifizieren
- nächste sinnvolle Schritte abzuleiten

Vereinbaren Sie ein unverbindliches Erstgespräch und erhalten Sie eine erste Einschätzung zu Ihrem Produkt im Kontext von CRA.

Jetzt Erstgespräch vereinbaren

steinel