# Cyber Resilience Act

***Nicht abwarten, sondern handeln***

*Autoren:*
*Philip Asmuth*
*Team Lead Security Architecture & Evaluation,*
*Denis Bock*
*Sales Manager Cybersecurity*
*achelos GmbH*
*www.achelos.de*

Mit dem Cyber Resilience Act (CRA) will die EU die wachsenden Risiken durch Cyberangriffe eindämmen und die Sicherheit digitaler Produkte auf ein einheitliches Niveau heben. Betroffen sind alle Hersteller von Hard- und Software mit digitalen Funktionen, die nun gefordert sind, die neuen Pflichten technisch wie organisatorisch umzusetzen. Spätestens im Dezember 2027 müssen die Vorgaben vollständig erfüllt sein. Die Umstellung wirkt auf den ersten Blick komplex – doch viele Anforderungen lassen sich mit etablierten Sicherheitsstandards und bewährten Verfahren erfüllen. Unternehmen können und sollten zeitnah damit beginnen.

## Die Zeit drängt

Ab dem 11. September 2026 müssen Unternehmen Schwachstellen in der IT-Sicherheit melden, ab dem 11. Dezember 2027, 36 Monate nach Inkrafttreten, sind sie verpflichtet, alle Anforderungen des Cyber Resilience Act (CRA) zu erfüllen, um weiterhin im europäischen Wirtschaftsraum verkaufen zu dürfen. Der CRA ist die Reaktion der EU auf verschiedenste Sicherheitsbedrohungen, die sich durch die Vernetzung und Digitalisierung der Gesellschaft ergeben: Spektakuläre Cyberattacken wie WannaCry, NotPetya und SolarWinds ereignen sich nun seit fast 15 Jahren, betreffen weltweit Unternehmen wie Behörden und richten massiven Schaden an.

Mit dem CRA will die EU Sicherheitsanforderungen für Produkte mit digitalen Elementen vereinheitlichen – mit dem Ziel, die Resilienz gegenüber Cyberattacken zu erhöhen. Der CRA ist eine Verordnung: Anders als eine Richtlinie gilt er in den EU-Mitgliedstaaten sofort ohne nationale Gesetzgebung. Er ist bereits am 11. Dezember 2024 in Kraft getreten.

## Was der CRA für Hersteller bedeutet

Hersteller von Produkten mit digitalen Elementen müssen gemäß CRA Anforderungen erfüllen, die sowohl die Produktsicherheit als auch die Herstellerprozesse betreffen.

Die Vorgaben zur Produktsicherheit regeln sowohl technische Merkmale als auch den sicheren Betrieb und die Kommunikation von Produkten. Gefordert wird unter anderem, dass Daten vertraulich und unverändert verarbeitet werden, dass unbefugter Zugriff verhindert wird und dass zentrale Funktionen auch unter Angriffsszenarien funktionsfähig bleiben. Darüber hinaus sollen mögliche Angriffsvektoren reduziert, Protokollierungs- und Überwachungsmechanismen eingerichtet und Sicherheitsupdates zuverlässig umgesetzt werden. Hinsichtlich ihrer internen Abläufe müssen Unternehmen Strukturen etablieren, um Schwachstellen systematisch zu erfassen, koordiniert zu beheben und Meldungen an zuständige Stellen wie die ENISA fristgerecht weiterzugeben.

## Lückenlose Dokumentation

Wichtig ist außerdem eine lückenlose Dokumentation der eingeführten Verfahren, da nur so die Erfüllung der Nachweispflichten möglich ist. Im Ergebnis reicht es also nicht aus, die reine Einhaltung formaler Vorgaben zu bestätigen – verlangt wird vielmehr der Nachweis funktionierender, in der Praxis gelebter Sicherheitsprozesse.

## Gültigkeit

Die CRA-Regelung erfasst alle Produkte, die digitale Funktionen enthalten – unabhängig davon, ob es sich um Hardware oder Software handelt. Betroffen sind Systeme, die Daten elektronisch verarbeiten und in Netzwerke eingebunden werden können. Der Anwendungsbereich reicht dabei von Alltagsgeräten wie Smartphones oder Webbrowsern über industrielle Steuerungstechnologien bis hin zu besonders sensiblen Bausteinen wie Smartcards oder Hardware-Sicherheitsmodulen.

## Unsicherheit bei der Umsetzung

So einfach lassen sich die CRA-Vorgaben aber nicht umsetzen: Viele Detailregeln fehlen noch oder werden erst kurz vor Beginn der verbindlichen Anwendung im Dezember 2027 erwartet. Hersteller müssen daher mit teils vagen und auslegungsbedürftigen Formulierungen arbeiten. So bleibt beispielsweise offen, wie genau die Integrität von Daten sicherzustellen ist oder welche Mechanismen für den Zugriffsschutz als ausreichend gelten. Der eigentliche Verordnungstext umfasst für diese Punkte kaum mehr als eine Seite, verweist aber auf noch zu erarbeitende harmonisierte Standards und Leitlinien der EU-Kommission.

## Einteilung

Diese Standards werden in folgende Kategorien gemäß dem New Legislative Framework eingeteilt:

- **Typ A („horizontale Frameworks“)** legen die übergreifenden Prinzipien und Begriffe fest, sind aber nicht produktspezifisch.
- **Typ B („horizontale Standards“)** formulieren generische Anforderungen und Prozessvorgaben, die produktunabhängig gelten.
- **Typ C („vertikale Standards“)** sind auf bestimmte Produktkategorien zugeschnitten, etwa Firewalls oder Steuerungssysteme, und sollen die Anforderungen vollständig abbilden.

## Zeitplan

Der Zeitplan sieht derzeit vor, dass ein erster Typ-A-Standard im August 2026 erscheint, gefolgt von 14 Typ-B-Standards zwischen September 2026 und Oktober 2027 sowie einem ersten Typ-C-Standard im Oktober 2026.

Auch die für die Auslegung entscheidenden Leitliniendokumente stehen noch aus. Lediglich ein Leitliniendokument zur Klassifizierung von Produkten hat bereits ein Veröffentlichungsdatum – den 11. Dezember 2025.

## Weitere Fragen

In weiteren Papieren sollen noch Fragen geklärt werden wie:

- Welche Pflichten ergeben sich aus der Nutzung von Open-Source-Komponenten?
- Wann gilt ein Produkt als wesentlich verändert?
- Und nach welchen Kriterien ist eine Risikobewertung vorzunehmen?

Wie hoch der Konformitätsnachweis sein muss, hängt von der Risikoklasse des Produkts ab, ob es sich um Alltagsprodukte, Komponenten mit Cybersecurity-Bezug oder Anwendungen in kritischen Infrastrukturen handelt. Für erstere ist nur eine Selbsterklärung notwendig, letztere benötigen eine externe Prüfung durch unabhängige Dritte.

## Handlungsempfehlung

Auch, wenn die Anforderungen auf den ersten Blick erschlagen: Unternehmen stehen beim CRA nicht völlig bei null. Zahlreiche technische wie organisatorische Vorgaben lassen sich durch bewährte Sicherheitsstandards und etablierte Vorgehensweisen abdecken – etwa durch die Normenreihe IEC 62443 oder branchenspezifische IoT-Standards. Wer sich frühzeitig an die Umsetzung macht, profitiert doppelt: Bestehende Prozesse können schon heute genutzt werden, und gleichzeitig werden spätere Engpässe bei Zeit und Kosten vermieden.

## Abwarten ist riskant

Warten, bis sämtliche Leitlinien und Standards endgültig vorliegen, ist riskant – sinnvoller ist es, jetzt die Grundlagen für die Umsetzung zu legen und zu beginnen. Ein zentrales Element ist dabei die verpflichtende Risikoanalyse des Produkts. Sie legt offen, was konkret geschützt werden muss, welche realistischen Bedrohungen existieren und wo die größten Schwachstellen liegen. Darauf lassen sich Schutzmaßnahmen zielgerichtet aufbauen.

Auch bei den internen Abläufen lohnt sich ein früher Einstieg. Viele prozessuale Anforderungen des CRA – etwa das Management von Schwachstellen – können schon heute in bestehende Strukturen integriert und weiterentwickelt werden, sodass die Konformität rechtzeitig erreicht wird.

## Fazit

Der Cyber Resilience Act wirkt auf den ersten Blick wie ein komplexes regulatorisches Labyrinth. Mit einer praxisnahen Herangehensweise lassen sich die Anforderungen jedoch gut meistern: Unternehmen können bestehende Standards und Best Practices nutzen und die Umsetzung aktiv angehen. Damit können sie nicht nur die Einhaltung der Vorschriften sicherstellen, sondern gleichzeitig ihre Widerstandsfähigkeit gegenüber den kontinuierlich wachsenden Cyberrisiken langfristig stärken.◄