Der EU Cyber Resilience Act (CRA): Was der neue CRA (auch Cyberresilienz-Verordnung) für Unternehmen bedeutet

Mit dem Cyber Resilience Act (CRA) hat die EU erstmals verbindliche Cybersicherheitsanforderungen für alle vernetzten Produkte geschaffen, die im EU-Binnenmarkt erhältlich sind. Hauptziel ist dabei die Stärkung der Cybersicherheit innerhalb der Europäischen Union. Die Verordnung trat bereits am 10. Dezember 2024 in Kraft und ist schrittweise bis zum 11. Dezember 2027 umzusetzen.

EU CYBER RESILIENCE ACT (CRA): WARUM DER CRA NOTWENDIG WURDE

Vernetzte Geräte und digitale Dienste spielen im Alltag eine immer größere Rolle - vom Smart-Home-System über industrielle IoT-Sensoren bis hin zu mobilen Apps. Verbraucher und Unternehmen nutzen mehr und mehr digitale Elemente. Mit dieser Vernetzung steigen aber auch die Risiken: Cyberangriffe nehmen zu und Sicherheitslücken in vernetzten Produkten können gravierende Folgen haben.

Der Cyber Resilience Act (Verordnung EU 2024/2847) ist die erste europäische Verordnung, die diese Gefahr bannen soll und ein Mindestmaß an Cybersicherheit für alle vernetzten Produkte festlegt, die auf dem EU-Markt erhältlich sind. Durch die Vorgaben aus dem CRA soll sichergestellt werden, dass Sicherheitslücken frühzeitig erkannt werden, Risiken minimiert und eine durchgehende Cybersicherheit über den gesamten Produktlebenszyklus gewährleisten werden kann.

Der CRA steht dabei in einem engen Zusammenhang mit der NIS2-Richtlinie. Beide zielen darauf ab, die Cybersicherheit in der EU zu stärken, setzen jedoch unterschiedliche Schwerpunkte. Der CRA konzentriert sich auf die Cybersicherheit von Produkten mit digitalen Elementen, indem verbindliche Sicherheitsanforderungen für Hardware und Software festgelegt werden, die in der EU hergestellt, importiert oder vertrieben werden.

Die NIS2-Richtlinie hingegen zielt auf die Verbesserung der Cybersicherheit von Netzwerken und Informationssystemen, die für wesentliche Dienste und kritische Infrastrukturen notwendig sind. Sie wendet sich daher an Betreiber wesentlicher Dienste und Anbieter digitaler Dienste. Beide Regelwerke ergänzen sich, um eine umfassende Cybersicherheitsstrategie für die EU zu gewährleisten.
Die CE-Kennzeichnung für Produkte mit digitalen Elementen wird künftig an die Konformität mit dem CRA geknüpft. Cybersicherheit wird damit zum integralen Bestandteil des Produktkonformitätsverfahrens.

RA Christian Geißler, LL.M.
Fachanwalt für IT-Recht
Wirtschaftsmediator (MuCDR)
christian.geissler@rdp-law.de

EU Cyber Resilience Act (CRA): Welche Wirtschaftsakteure betroffen sind

Der CRA gilt nicht nur für die Hersteller digitaler Produkte, sondern verpflichtet alle Wirtschaftsakteure in der Lieferkette. Hersteller, Importeure und Händler müssen die Einhaltung des CRA sicherstellen. Auch außereuropäische Unternehmen sind nicht ausgenommen. Möchte ein Unternehmen die eigenen Produkte auf dem EU-Markt vertreiben, so müssen die Anforderungen des CRA eingehalten werden.

Welche Produkte betrifft der CRA?

Der CRA gilt für alle sogenannten „Produkte mit digitalen Elementen". Darunter versteht man Produkte, die direkt oder indirekt mit einem Gerät oder Netzwerk verbunden werden können (sog. „Datenfernverarbeitungslösungen"). Das umfasst sowohl vernetzte Hardware als auch reine Softwareprodukte: Smartphones, Laptops, Smart-Home-Produkte, Smartwatches, vernetztes Spielzeug, Router, Firewalls, Mikroprozessoren, Smartcards, mobile Apps, Computerspiele oder Antivirenprogramme.

Ausnahmen vom CRA: Nicht-kommerzielle Open-Source-Software, Medizinprodukte, Fahrzeuge, Produkte der zivilen Luftfahrt und Schiffsausrüstung sowie Cloud-Computing-Dienste und Software-as-a-Service (SaaS).

EU Cyber Resilience Act (CRA): Welche Pflichten der CRA für Produkte vorsieht

Der CRA teilt Produkte nach ihrem Sicherheitsrisiko in verschiedene Kategorien ein. Je nach Kategorie gelten unterschiedliche Konformitätsbewertungsverfahren. Unter einem Konformitätsbewertungsverfahren versteht man die Prüfung, ob ein Produkt die Vorgaben aus dem CRA (und ggf. anderer Rechtsnormen) einhält oder nicht. Je nach Produktkategorie reicht entweder eine Selbstbewertung oder es ist eine umfassende Qualitätssicherung durch eine sogenannte notifizierende Stelle notwendig.
Für alle Produkte mit digitalen Elementen, egal ob billig oder teuer, ob für Verbraucher oder für Geschäftsanwender, gelten aber dieselben grundlegenden Cybersicherheitsanforderungen.

Produktkategorien und Risikoklassen im Cyber Resilience Act

Standardprodukte: Die Mehrheit aller betroffenen Produkte fällt in diese Kategorie (z.B. Smart-Home-Systeme, einfache IoT-Sensoren, etc.). Hier ist eine Selbstbewertung durch den Hersteller ausreichend.

Eine weitere Kategorie sind die sogenannten „Wichtigen Produkte". Für diese werden dann sogar zwei unterschiedliche Klassen eingeführt. Unter die Klasse I der wichtigen Produkte fallen Produkte wie Passwortmanager, Netzwerkmanagementsysteme oder Antivirensoftware. Diese können vom Hersteller selbst bewertet werden, sofern harmonisierte Normen angewendet werden. Andernfalls ist eine externe Bewertung erforderlich.

RA Christian Geißler, LL.M.
Fachanwalt für IT-Recht
Wirtschaftsmediator (MuCDR)
christian.geissler@rdp-law.de

Wichtige Produkte der Klasse II sind Firewalls, Container-Runtime-Systeme oder manipulationssichere Mikroprozessoren. Für diese Produkte ist eine Konformitätsbewertung durch eine notifizierte Stelle zwingend erforderlich.

Die letzte Kategorie sind die sogenannten „Kritischen Produkte“: Darunter fallen z.B. Produkte wie Smartcards oder Smart-Meter-Gateways, die für Sicherheitszwecke in kritischen Infrastrukturen eingesetzt werden. Hier ist eine Zertifizierung nach einem europäischen Zertifizierungsschema verpflichtend.

EU Cyber Resilience Act (CRA): Welche Pflichten Hersteller erfüllen müssen

Der CRA stellt umfassende Anforderungen an Hersteller, die während des gesamten Lebenszyklus eines Produktes gelten.

Es gelten die Konzeptionsgrundsätze „Secure by Design“ und „Secure by Default“. Bereits während der Produktentwicklung muss Cybersicherheit berücksichtigt werden. Vernetzte Produkte müssen unter anderem so konzipiert sein, dass Daten verschlüsselt werden und die Angriffsfläche minimal ist. Standardeinstellungen müssen zur Sicherheit beitragen - etwa durch das Verbot schwacher Standardpasswörter.

Die Hersteller müssen eine sogenannte Software Bill of Materials (SBOM) erstellen. Das heißt es muss eine Software-Entwicklungsliste erstellt werden, die alle verwendeten Softwarekomponenten oder verwendeten Bibliotheken dokumentiert. Diese soll wesentlich für das Schwachstellenmanagement sein, muss aber nicht veröffentlicht werden.

Produkte erhalten eine neue Konformitätserklärung zu den Cybersicherheitsanforderungen. Je nach Produktkategorie muss das Konformitätsbewertungsverfahren durchgeführt werden an dessen Ende eine Erklärung steht, ob und inwiefern die Vorgaben des CRA eingehalten werden. Die bisher schon notwendige CE-Kennzeichnung wird um diese neue Konformitätserklärung erweitert.

Der CRA macht neue Vorgaben zum Schwachstellenmanagement und notwendigen Softwareupdates. Während des gesamten Supportzeitraums (in der Regel fünf Jahre) müssen Hersteller Schwachstellen zukünftig aktiv handhaben und kostenlose Sicherheitsupdates bereitstellen.

Zuletzt werden Meldepflichten eingeführt. Aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle müssen über die zentrale ENISA-Meldeplattform gemeldet werden. Zunächst muss eine sogenannte Frühwarnung innerhalb von 24 Stunden erfolgen, sodann müssen weitere Informationen innerhalb von 72 Stunden und ein Abschlussbericht nach 14 Tagen bzw. einem Monat eingereicht werden.

RA Christian Geißler, LL.M.
Fachanwalt für IT-Recht
Wirtschaftsmediator (MuCDR)
christian.geissler@rdp-law.de

Umsetzungsfristen und Zeitplan des CRA

Bereits zum 10. Dezember 2024 ist der CRA In-Kraft getreten.
Ab dem 11. Juni 2026 sind die sogenannten Konformitätsbewertungsstellen berechtigt Produkte zu bewerten.
Ab dem 11. September 2026 müssen die Meldepflichten für Schwachstellen und Sicherheitsvorfälle eingehalten werden.
Schließlich gelten ab dem 11. Dezember 2027 auch alle übrigen Anforderungen des CRA vollständig.

Cyber Resilience Act (CRA): Sanktionen und Bußgelder

Wie auch bei anderen Verordnungen kann auch die Nichteinhaltung des CRA erhebliche Sanktionen für ein betroffenes Unternehmen nach sich ziehen.
Bei Verstößen können Bußgelder von bis zu 15 Millionen Euro oder 2,5 Prozent des weltweiten Jahresumsatzes - je nachdem, welcher Betrag höher ist – verhängt werden.

Darüber hinaus kann die zuständige Behörde auch Marktzugangsbeschränkungen verhängen. Das kann zur Folge haben, dass der Verkauf von nicht konformen Produkten in der EU eingeschränkt oder sogar vollständig verhindert werden kann. Ein Produkt ist nämlich nur dann für den europäischen Markt zugelassen, wenn es den CRA-Anforderungen entspricht.

Es können sogar Produktrückrufe angeordnet werden. Das bedeutet, in schwerwiegenden Fällen kann eine vollständige Rücknahme oder ein Rückruf des Produkts vom Markt verlangt werden. Die Marktüberwachungsbehörden werden durch den CRA sogar ermächtigt aktiv nach Verstößen zu suchen und entsprechende Maßnahmen durchzusetzen.

Fazit: Warum der EU Cyber Resilience Act (CRA) die Cybersicherheit grundlegend verändert

Der Cyber Resilience Act soll einen Paradigmenwechsel für die Cybersicherheit vernetzter Produkte in Europa markieren. Zwar bedeutet er für Unternehmen neue Herausforderungen, aber zugleich auch Chancen. Unternehmen die frühzeitig in Cybersicherheit investieren stärken das Vertrauen in die eigenen Produkte und verschaffen sich Wettbewerbsvorteile.

Angesichts empfindlicher Strafen und der Meldepflichten, die zum Teil bereits ab September 2026 gelten, ist aber ohnehin proaktives Handeln zu empfehlen. Der CRA ist daher nicht nur regulatorische Pflicht – er kann auch eine Investition in die Zukunftsfähigkeit digitaler Produkte darstellen.

RA Christian Geißler, LL.M.
Fachanwalt für IT-Recht
Wirtschaftsmediator (MuCDR)
christian.geissler@rdp-law.de

EU Cyber Resilience Act (CRA) – FAQ für Unternehmen

Was ist der EU Cyber Resilience Act (CRA)?

Der EU Cyber Resilience Act (CRA) ist eine europäische Verordnung, die verbindliche Cybersicherheitsanforderungen für Produkte mit digitalen Elementen festlegt. Ziel ist es, Sicherheitslücken zu reduzieren und ein einheitliches Cybersicherheitsniveau im EU-Binnenmarkt zu schaffen.

Seit wann gilt der Cyber Resilience Act?

Der CRA ist am 10. Dezember 2024 in Kraft getreten. Die vollständige Anwendung aller Vorgaben ist jedoch erst ab dem 11. Dezember 2027 verpflichtend.

Für wen gilt der EU Cyber Resilience Act?

Der CRA gilt für:

- Hersteller digitaler Produkte
- Importeure
- Händler

Dies betrifft auch Nicht-EU-Unternehmen, sobald ihre Produkte im europäischen Markt angeboten werden.

Welche Produkte fallen unter den Cyber Resilience Act?

Der CRA gilt für alle Produkte mit digitalen Elementen, darunter fallen z.B.:

- vernetzte Hardware (z. B. Router, Smart-Home-Geräte, IoT-Produkte)
- Software (z. B. Apps, Betriebssysteme, Antivirensoftware, Computerspiele)

Welche Produkte sind vom CRA ausgenommen?

Ausgenommen sind u. a.:

- nicht-kommerzielle Open-Source-Software
- Medizinprodukte
- Fahrzeuge
- Produkte der zivilen Luftfahrt und Schiffsausrüstung
- Cloud-Computing-Dienste und SaaS-Angebote

Gelten für alle Produktkategorien dieselben Vorgaben?

Der Cyber Resilience Act unterscheidet Produkte nach sogenannten Risikoklassen, wonach für die betreffenden Produkte unterschiedliche Pflichten bestehen:

- Standardprodukte (Selbstbewertung)
- Wichtige Produkte – Klasse I (teilweise Selbstbewertung)
- Wichtige Produkte – Klasse II (externe Konformitätsbewertung)

RA Christian Geißler, LL.M.
Fachanwalt für IT-Recht
Wirtschaftsmediator (MuCDR)
christian.geissler@rdp-law.de

- Kritische Produkte (EU-weite Zertifizierungspflicht)

Welche Pflichten haben Hersteller nach dem CRA?

Hersteller müssen u. a.:

- Cybersicherheit nach dem Prinzip Secure by Design & Secure by Default umsetzen
- eine Software Bill of Materials (SBOM) erstellen
- Sicherheitslücken aktiv managen
- kostenlose Sicherheitsupdates bereitstellen
- eine CRA-Konformitätserklärung abgeben

Was ist eine Software Bill of Materials (SBOM)?

Die SBOM ist eine Übersicht aller eingesetzten Softwarekomponenten. Sie dient dem Schwachstellenmanagement und ist verpflichtend zu erstellen, muss aber nicht öffentlich zugänglich gemacht werden.

Welche Meldepflichten bestehen nach dem Cyber Resilience Act?

Schwerwiegende Sicherheitsvorfälle müssen über die ENISA-Meldeplattform gemeldet werden:

- Frühwarnung innerhalb von 24 Stunden
- Detailmeldung innerhalb von 72 Stunden
- Abschlussbericht nach spätestens einem Monat

Ab wann gelten die Meldepflichten?

Die Meldepflichten nach dem CRA gelten ab dem 11. September 2026.

Welche Bedeutung hat der CRA für die CE-Kennzeichnung?

Die CE-Kennzeichnung wird an die Einhaltung der CRA-Cybersicherheitsanforderungen geknüpft. Ohne CRA-Konformität ist ein Vertrieb im EU-Markt nicht mehr zulässig.

Welche Sanktionen drohen bei Verstößen gegen den CRA?

Bei Verstößen drohen:

- Bußgelder bis zu 15 Mio. EUR oder 2,5 % des weltweiten Jahresumsatzes
- Verkaufsverbote
- Marktzugangsbeschränkungen
- Produktrückrufe

Wie unterscheidet sich der CRA von der NIS2-Richtlinie?

Der Cyber Resilience Act regelt die Sicherheit von Produkten,
die NIS2-Richtlinie die Sicherheit von Netzwerken und Diensten.
Beide Regelwerke ergänzen sich, verfolgen aber unterschiedliche Ansätze.

RA Christian Geißler, LL.M.
Fachanwalt für IT-Recht
Wirtschaftsmediator (MuCDR)
christian.geissler@rdp-law.de