Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Cyber Resilience Act – Cybersicherheit EU-weit gedacht

Was ist der Cyber Resilience Act (CRA)?

*Der **Cyber Resilience Act** ist die erste europäische Verordnung, die ein Mindestmaß an Cybersicherheit für alle vernetzten Produkte festlegt, die auf dem EU-Markt erhältlich sind – etwas, das es bisher nicht gab. Ziel ist es, die Cybersicherheit innerhalb der Europäischen Union zu erhöhen. Die neuen Vorschriften gelten in allen EU-Mitgliedstaaten und werden schrittweise umgesetzt.*

Wann geht es los?

20 Tage nach der Veröffentlichung im Amtsblatt der EU tritt der CRA in Kraft. Die Umsetzung erfolgt in verschiedenen Etappen, bis Ende 2027 alle Anforderungen von neuen Produkten erfüllt werden müssen.

Fällt mein Produkt unter den CRA?

Mein Produkt:

- verwendet digitale Elemente oder ist ein Softwareprodukt
- wird ab Ende 2027 neu auf den EU-Markt gebracht
- ist nicht explizit bei den fünf Ausnahmesektoren genannt (Medizinprodukte, Fahrzeuge, In-vitro-Diagnostika, zivile Luftfahrt sowie Produkte im Kontext der nationalen Sicherheit)
- ist keine kostenfreie Open-Source-Software ohne Gewinnerzielungsabsicht

Ich muss den CRA anwenden.

KMU oder Start-up – was ist mit uns?

Unterstützung für kleine und mittlere Unternehmen, Kleinstunternehmen (KMU) und Start-ups ist direkt im CRA vorgesehen. Unter anderem wird es Leitlinien für die Umsetzung geben, werden Helpdesks für die Unterstützung bei den Meldepflichten zur Verfügung stehen, die technische Dokumentation kann sich vereinfachen und es werden Regulatory Sandboxes für die Überprüfung von Produkten mit digitalen Elementen eingerichtet.

23.10.2024
Verabschiedung des CRA

20.11.2024
Veröffentlichung des Gesetzestextes im Europäischen Amtsblatt

Was ist zu tun?

1. Cybersicherheit mitdenken

Während der Produktentwicklung sollten die Anforderungen des CRA bedacht werden. Hersteller müssen eine **Risikobewertung** durchführen und die Grundsätze **„security by design“** und **„security by default“** berücksichtigen. Sie sollten Tools zur Erstellung von **Software Bill of Materials (SBOM)** integrieren.

2. Anforderungen nachweisen

Eine **Konformitätserklärung** wird benötigt, um nachzuweisen, dass das Produkt alle Anforderungen des CRA erfüllt. Welches Konformitätsbewertungsverfahren infrage kommt, hängt von der Produktkategorie ab.

3. Schwachstellen offenlegen

Für den leichten **Informationsaustausch zu Schwachstellen** sowie schwerwiegenden Sicherheitsvorfällen wird eine neue zentrale Meldeplattform etabliert.

4. Sicher im gesamten Supportzeitraum

Während des gesamten Produktlebenszyklus müssen für den Endanwender **Security Updates** zur Verfügung gestellt und das Schwachstellenhandling betrieben werden. Dieser Supportzeitraum beträgt in der Regel fünf Jahre.

SBOM – „Zutatenliste“ für Software

Eine SBOM ist für Software das Äquivalent zum Zutatenverzeichnis für Lebensmittel. Sie detailliert, welche Bibliotheken und weitere Softwarekomponenten im Produkt benutzt werden. Der CRA schreibt das Erstellen einer SBOM vor, sie muss jedoch nicht veröffentlicht werden.

Standard, wichtig oder kritisch – was trifft zu?

Die meisten Produkte, für die der CRA relevant ist, sind Standardprodukte. Nur Produkte, die unter dem Gesichtspunkt der Cybersicherheit als sensibler gelten, werden als „wichtige“ oder „kritische“ Produkte bezeichnet und sind in den Anhängen III und IV der Verordnung aufgeführt (z. B. Passwortmanager, Firewalls, Smartcards, intelligente Zähler usw.).

11.12.2024
Der CRA tritt in Kraft

11.06.2026
Konformitätsbewertungsstellen können die Erfüllung der Anforderungen an den CRA bewerten

11.09.2026
Meldepflicht für Schwachstellen und Sicherheitsvorfälle

11.12.2027
Alle CRA-Anforderungen sind bei neuen Produkten eingehalten

Wie unterstützt das BSI?

Um die Anforderungen des CRA greifbarer zu machen, erarbeitet das BSI eine Technische Richtlinie, in der die Anforderungen an Hersteller und Produkte hinsichtlich der Cyberresilienz übersichtlich und konkret beschrieben sind.

In Teil 1 „General Requirements“ werden Anforderungen an Hersteller und Produkte in Anlehnung an die Anforderungen aus Artikeln und Anhängen des CRA zusammengestellt, in Teil 2 „Software Bill of Materials (SBOM)“ formelle und fachliche Vorgaben für SBOMs. Teil 3 „Vulnerability Reports and Notifications“ beschreibt den Umgang mit eingehenden Schwachstellenmeldungen.

Generelles:

Bitte beachten Sie, dass die hier gegebenen Hinweise nur zu Informationszwecken dienen und nicht als Rechtsberatung gedacht sind. Der Rechtstext des CRA hat Vorrang vor den hier gegebenen Erläuterungen.

Informationen zur Technischen Richtlinie

Weitere Informationen und ein FAQ gibt es auf der BSI-Webseite zum CRA

Impressum

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: 0800 274 1000
E Mail: bsi@bsi.bund.de
www.bsi.bund.de

Bildnachweis Adobe Stock/ your123

Stand November 2024