Produktanforderung

- Angemessenes Cybersicherheitsniveau auf Basis einer Risikobewertung
- Cybersicherheit als Teil des Design-, Entwicklungs- und Produktionsprozesses (Security-by-Design)
- Sichere Grundkonfiguration (Security-by-Default)
- Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit des Produktes

Anforderungen zum Umgang mit Schwachstellen

- Entgegennahme von Schwachstellenmeldungen und Durchführung regelmäßiger Sicherheitstests
- Angemessene Behandlung von Schwachstellen
- Bereitstellung von kostenlosen Sicherheits-Updates begleitet von Hinweismeldungen an Nutzende
- Öffentliche Informationen über Schwachstellen und ihre Behebung

(Dritt-)Komponenten und sichere Lieferkette

- Software Bill of Materials (SBOM) erfasst (Dritt-)Komponenten
- Sorgfaltspflicht bei der Verwendung von (Dritt-)Komponenten
- Nachverfolgung und Weiterleitung möglicher Schwachstellen an Lieferanten

Mindestinformation von Herstellern an Nutzende

- Kontaktstelle für Informationen über Schwachstellen
- Information zur Produktidentifizierung (Typ, Version etc.)
- Angaben über die bestimmungsgemäße Verwendung
- Zugriffsmöglichkeiten auf die EU-Konformitätserklärung und falls verfügbar SBOM

Wann ist was zu tun?

Risikobewertung eines Produkts

(1) Produktbezogene Anforderungen
(2) Anforderungen in Bezug auf den Umgang mit Schwachstellen
(3) Technische Dokumentation

Konformitätsbewertung, CE-Kennzeichen, EU-Konformitätserklärung

Kontinuierliche Einhaltung der Anforderungen während des gesamten Supportzeitraums

Design- und Entwicklungsphase

Wartungsphase
(mindestens 5 Jahre ab Inverkehrbringen; ggf. kürzer oder länger, sofern zu erwarten ist, dass die Zeit, in der das Produkt verwendet wird, kürzer/länger ist)

Meldepflichten

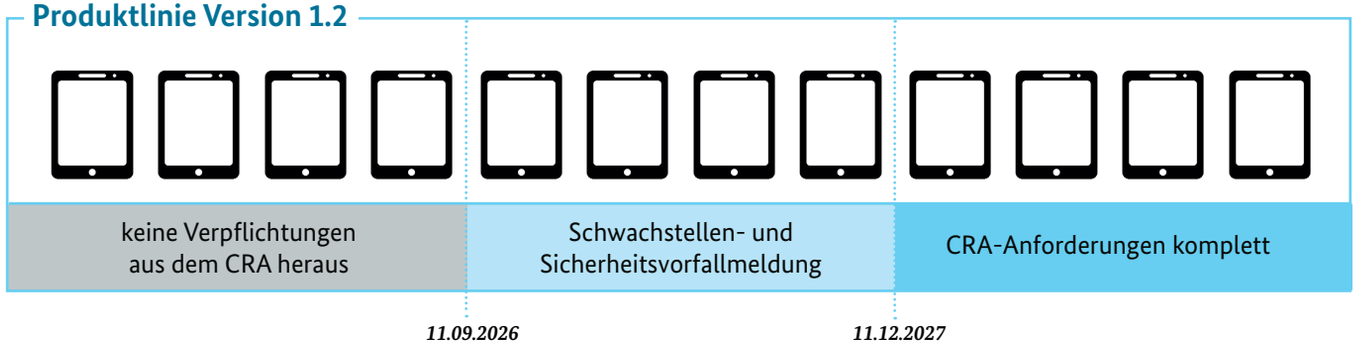
Cyber Resilience Act – CRA

Wie mache ich meine Produkte fit für eine (cyber-) sichere Zukunft?

Bundesamt
für Sicherheit in der
Informationstechnik

Wann muss ein Produkt welche Anforderungen des Cyber Resilience Acts erfüllen?

- Für **alle** Produkte mit digitalen Elementen einschließlich reiner Softwareprodukte[1] gilt ab 11.09.2026: aktiv ausgenutzte Schwachstellen und schwere Sicherheitsvorfälle bei zentraler Meldeplattform **melden**.
- Alle **neuen** Produkte mit digitalen Elementen[1] müssen ab 11.12.2027 den **CRA komplett erfüllen**.
- Produkte mit digitalen Elementen[1], die ab dem 11.12.2027 wesentlich **geändert** werden, müssen den **CRA** nach der Aktualisierung **komplett erfüllen**.
- Betrifft jedes einzelne Produkt, das nach dem 11.12.2027 in der EU in Verkehr gebracht wird, auch wenn das Produktmodell oder die Produktart bereits vor dem Inkrafttreten des CRA bereitgestellt wurde.[2]



[1] Außer bereits anderweitig durch EU regulierte Produkte, Produkte der nationalen Sicherheit sowie nicht kommerzielle Open Source Software.

[2] Vergleiche hier Blue-Guide 2.3. Inverkehrbringen (Leitfaden für die Umsetzung der Produktvorschriften der EU 2022).

CRA – jetzt schon mitdenken!

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

Informationen zur Technischen Richtlinie

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.

Impressum

Herausgeber
Bundesamt für Sicherheit
in der Informationstechnik
Postfach 20 03 63
53133 Bonn

E Mail: bsi@bsi.bund.de

Stand
09/2025

Druck
Appel & Klinger Druck und Medien GmbH
www.ak-druck medien.de

Bildnachweis
Yuichiro Chino/Getty Images