HISOLUTIONS

Cyber Resilience Act (CRA): Neue EU-Vorgaben für digitale Produkte

Wie der CRA Produktsicherheit, Verantwortlichkeiten und Prozesse verändert

Know-how to go I 10. Juni 2026

Jan Klose

Jan Klose
Consultant

- Beratung und Begleitung von Unternehmen bei der Einführung und Verbesserung ihrer Informationssicherheitsmanagementsysteme
- Koordination der Informationssicherheit in der Rolle des ISB
- Durchführung von Strukturanalysen, Schutzbedarfsfeststellungen und Risikoanalysen
- Beratung und Durchführung von Gap-Analysen zum CRA

Der CRA setzt neue Standards für Cybersicherheit

- **EU-weite Cybersicherheitsstandards** für digitale Produkte (Hardware & Software) zur Stärkung der digitalen Sicherheit
- **Pflichten für Hersteller:** Sicherheitskonzepte wie „Security by Design“ und regelmäßige Updates über den gesamten Produktlebenszyklus
- **Transparenz & Meldepflicht:** Software-Stückliste (SBOM) und Meldung von Sicherheitsvorfällen innerhalb von 24 Stunden
- **Umsetzung & Sanktionen:** Inkrafttreten seit Dez. 2024, vollständige Anwendung bis Dez. 2027; bei Verstößen drohen Geldstrafen und Verkaufsverbote

Aktueller Status

Bisherige Fortschritte

Überwachen, verfolgen und über den Fortschritt neuer Initiativen, Ergebnisse und Rechtsvorschriften auf dem Laufenden bleiben.

Quelle: Europäische Kommission https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation, Stand 27. Mai 2026

Cybersicherheit wird Pflicht

Wer Produkte mit digitalen Elementen in der EU auf den Markt bringt, muss …

- sie sicher entwickeln,
- einen sicheren Betrieb ermöglichen,
- Schwachstellen behandeln,
- relevante Vorfälle melden.

Produkte, die unter den CRA fallen

Kommerziell vertriebene Produkte mit Software- oder Hardware-Komponenten, die direkte oder indirekte Datenverbindungen zu anderen Geräten oder Netzwerken haben.

Fällt darunter

- Smart-Home-Geräte
- Router & Firewalls
- Industriesteuerungen
- Betriebssysteme
- Smartphone-Apps
- Bibliotheken & SDKs
- Spielzeug mit Vernetzung

Fällt NICHT darunter

- Reine Dienstleistungen (SaaS)*
- Medizinprodukte (eigene Regulierung)
- Luftfahrt (eigene Regulierung)
- Fahrzeuge (eigene Regulierung)
- Nationale Sicherheit/Militär
- Open Source (nicht-kommerziell)

*Achtung: Cloud-Dienste, die Teil eines Produkts sind (z. B. Backend einer App), fallen MIT unter den CRA!

Produktkategorien bestimmen die Konformitätsbewertung

Kritikalität

Produktkategorie	Beispiele
Standard ▪ Eigenerklärung / interne Fertigungskontrolle → ohne notifizierte Stelle	• Mobile Apps • Smart Speaker • Computerspiele • digitale Haushaltsgeräte
Wichtig ▪ **Klasse I** ▪ Wie **Standard** bei vollständiger Anwendung harmonisierter Normen / Spezifikationen / Zertifizierung → sonst wie **Klasse II** ▪ **Klasse II** ▪ EU-Baumusterprüfung + interne Fertigungskontrolle ▪ oder umfassende Qualitätssicherung → mit notifizierte Stelle	• Passwortmanager • Betriebssysteme • Router • VPN • Browser • Hypervisoren • Firewalls • IDS/IPS
Kritisch ▪ EU-Cybersicherheitszertifikat, mind. „mittel“, wenn von EU vorgegeben und Schema vorhanden → sonst wie **Klasse II**	• Security Boxes • Smart-Meter-Gateways • Smartcards/Secure Elements

Der Hersteller trägt die Hauptverantwortung

Hersteller

- Security-Anforderungen umsetzen
- Schwachstellen behandeln
- Dokumentation/CE/ Konformität
- Meldepflichten einhalten

Hauptverantwortung

Importeure

- Prüfen, ob der Hersteller seine Pflichten erfüllt hat
- Nur konforme Produkte in Verkehr bringen

Händler

- Dürfen keine offensichtlich nicht-konformen Produkte vertreiben
- Bei Risiken Meldung weitergeben

Open Source verbaut? Produkt verkauft? Dann liegen die CRA-Herstellerpflichten grundsätzlich beim Anbieter des Endprodukts.

Kernpflichten für Hersteller

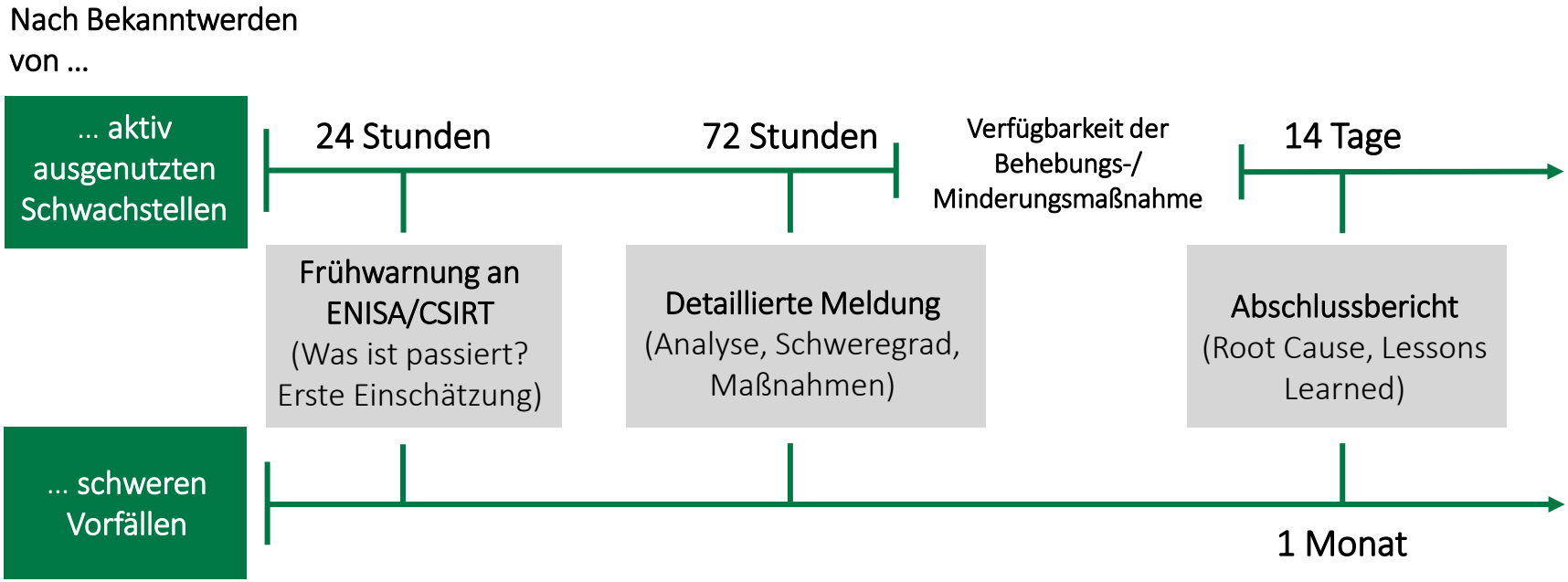
VOR dem Inverkehrbringen

- Cybersecurity-Risikobewertung durchführen
- Security by Design – sichere Architektur & Entwicklung
- Technische Dokumentation erstellen
- Konformität bewerten/bewerten lassen (je nach Klasse)
- CE-Kennzeichnung anbringen
- Sicherheitsinformationen für Nutzer bereitstellen

NACH dem Inverkehrbringen (über den gesamten Support-Zeitraum)

- Sicherheitsupdates bereitstellen (mind. 5 Jahre oder Produktlebensdauer)
- Schwachstellen aktiv identifizieren und beheben
- Meldepflichten einhalten
- SBOM (Software Bill of Materials) pflegen

Erste Pflichten gelten schon ab 11. September 2026 (Meldepflichten)



Gilt für **alle** Produktkategorien

Die CRA-Vorbereitung beginnt schon vor der vollständigen Anwendung

Zentrale Handlungsfelder für Hersteller

Betroffene Produkte identifizieren
Produktportfolio prüfen und CRA-relevante Hardware, Software und vernetzte Komponenten erfassen

Risikobewertung etablieren
Cybersecurity-Risiken systematisch über den gesamten Produktlebenszyklus bewerten

Security by Design verankern
Sicherheitsanforderungen früh in Entwicklung, Architektur und Standardkonfigurationen integrieren

Vulnerability Management aufsetzen
Prozesse für Schwachstellenmanagement, Patches und Updates definieren

SBOM und Transparenz vorbereiten
Software-Komponenten und Abhängigkeiten strukturiert dokumentieren

Technische Dokumentation standardisieren
Nachweise zu Sicherheitsanforderungen, Tests, Updates und Support sauber aufbauen

Meldeprozesse vorbereiten
Interne Abläufe für die fristgerechte Meldung von Schwachstellen und Sicherheitsvorfällen festlegen

Supportzeiträume definieren
Klare Regelungen für Update- und Wartungszeiträume je Produkt schaffen

Konformitätsbewertung früh planen
Produktkategorien und passende Bewertungsverfahren rechtzeitig einordnen

Kontakt

Jan Klose
Consultant