Herzlich Willkommen

CRA für Anwender

Wie Unternehmen künftig sicherere Soft- und Hardware beschaffen können

Paolo Magrini

Georg Janko

BIHK-Reihe zur
IT-Sicherheit, 03.09.2026

hvs consulting



Wer wir sind



Paolo Magrini

Information Security Consultant
Schwerpunkt auf Sicherheit aus regulatorischer Sicht

E-Mail paolo.magrini@hvs-consulting.de
Web www.hvs-consulting.de



Georg Janko

Information Security Consultant
Schwerpunkt auf Sicherheit aus Anwendersicht

E-Mail georg.janko@hvs-consulting.de
Web www.hvs-consulting.de

Agenda

1. Was ist der CRA?
2. Wer sind die Anwender?
3. CRA aus Anwendersicht





Was ist der Cyber Resilience Act?

Was ist der Cyber Resilience Act (CRA)?

hvs consulting

Verordnung (EU) 2024/2847 — in Kraft seit 10. Dezember 2024

Keine Richtlinie – eine Verordnung



- Gilt in allen 27 EU-Staaten.
- Kein nationales Umsetzungsgesetz nötig (im Gegensatz zu NIS-2).

Gilt für Hersteller weltweit



Wer digitale Produkte im EU-Markt verkauft, egal ob aus München, Tokyo oder San Francisco, muss CRA-konform sein.

Gesamter Produktlebenszyklus



- Security by Design & Default
- Aktives Schwachstellen-management
- Kostenlose Sicherheits-Updates über den gesamten Supportzeitraum.

EU-Verordnung mit verbindlichen Mindestanforderungen an Sicherheit für alle Produkte mit digitalen Elementen

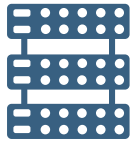
Wen betrifft der CRA?

hvs consulting

Produkte mit digitalen Elementen



Software und Apps
Betriebssysteme, Apps, SaaS-Clients, Computerspiele



Vernetzte Hardware
Router, Firewalls, Smartmeter, Industriesteuerungen, Sensoren mit Netzwerkschnittstelle



IoT & Verbraucherprodukte
Smart-Home, Wearables, Smartphones, vernetzte Spielzeuge



B2B-Systemhersteller
Maschinen-und Anlagenbauer mit vernetzten Steuerungen

Ausnahmen

Medizinprodukte

KFZ & Fahrzeugsysteme

Luft- und Raumfahrt (EASA)

Marine-Ausrüstung

Militär & nationale Sicherheit

Nicht-kommerziell genutzte Open-Source-SW

Browserbasierte SaaS

Produktkategorien & Klassifizierung

hvs consulting

Standard Produkte	Wichtige Produkte Klasse I	Wichtige Produkte Klasse II	Kritische Produkte
Konformitätsnachweis: Selbstbewertung	**Konformitätsnachweis:** Ggf. Selbstbewertung / Drittstellenprüfung	**Konformitätsnachweis:** Drittstellenprüfung	**Konformitätsnachweis:** Strenge Drittstellenprüfung
Beispiele Smart-Home Geräte, Bluetooth-Lautsprecher, Spiele, Buchhaltungssoftware, etc.	**Beispiele** Betriebssysteme, Router, Browser, Passwort-Manager, VPN-Produkte, etc.	**Beispiele** Industrielle Firewalls, Hypervisoren, etc.	**Beispiele** Smart-Meter, Hardware-Sicherheitsmodule, Smartcards, etc.

Je höher das Risikopotenzial, desto strenger die Prüfpflicht

Durchführungsverordnung (EU) 2025/2392 vom November 2025 konkretisiert die Kategoriezuordnung je Produktkategorie.

Was verlangt der CRA konkret?

hvs consulting

Pflichten für Hersteller, Importeure, Händler

Security by Design & Default

Sicherheit muss von Beginn der Entwicklung eingebaut sein durch z.B. Security by Design, Threat Modelling

Schwachstellen Management

Systematische Risikoanalyse, proaktives Monitoring der Komponenten und bekannter Lücken

Dokumentation

Von Schwachstellen, Sicherheitsmaßnahmen, eingesetzter Softwarekomponenten (SBOM)

Meldepflicht

Bei aktiv ausgenutzen Schwachstellen oder schweren Sicherheitsvorfällen innerhalb von 24h

Sicherheitsupdates

Müssen kostenlos über den vom Hersteller angegebenen Supportzeitraum bereitgestellt werden

CE-Kennzeichnung

Ab Dezember 2027 nur noch Marktzugang mit CE-Zeichen für Cybersicherheit

Fristen & Zeitplan

hvs consulting

Registrierung im ENISA Portal erst ab 11.09 möglich

CRA tritt in Kraft

10. Dezember 2024

Prüfstellen werden benannt

(Konformitäts-bewertungsstellen), die die Konformität des Produktes übernehmen sollen, können bekannt gemacht werden.

11. Juni 2026

Meldepflicht für Hersteller

Hersteller müssen ausgenutzte Schwachstellen innerhalb von 24 Std. melden

Meldung über die von der ENISA bereitgestellte Single Reporting Platform (SRP)

11. September 2026

CRA gilt vollumfänglich

- Produkt ist CRA-konform
- CE-Label
- Dokumentation

11. Dezember 2027



Wer sind die Anwender?

Wer sind die Anwender? Unternehmen / Anwender

hvs consulting



Unternehmen

- Hersteller (z.B. Software-Entwickler)
- Händler
- Importeure



Anwender

- Geschäfts-/Bereichsleitung
- Produkt-/Qualitätsmanagement
- Forschung & Entwicklung
- Einkauf / Lieferketten
- Produktentwicklung & -sicherheit
- Informationssicherheitsverantwortliche



CRA aus Anwendersicht

Was ändert sich für Anwender?

hvs consulting



Neue Garantien

- Konformitätserklärung mit dem CRA
- Sicherheitsupdates über definierte Zeiträume
- Sichere Standardeinstellungen
- Meldewege für Schwachstellen
- Klare Herstellerverantwortung



Zusätzliche Informationen

- Technische Sicherheitsdokumentation
- Sicherheitsbewertung
- Informationen zu Supportzeiträumen
- Nutzerinformationen
- Angaben zu Abhängigkeiten

Was ändert sich für Anwender?

Anwender

Geschäfts-/Bereichsleitung

Produkt-/Qualitätsmanagement

Forschung & Entwicklung

Einkauf / Lieferketten

Produktentwicklung & -sicherheit

Informationssicherheitsverantwortliche



Was ändert sich für Anwender?

Geschäfts-/Bereichsleitung

- Besserer Überblick über **Produktrisiken**
- Bessere **Entscheidungsgrundlagen**
- **Verantwortung** sichere Produkte zu beziehen

Was ändert sich für Anwender?

Produkt-/Qualitätsmanagement

- **Sicherheitsanforderungen** klarer bewertbar
- Mehr Einblick in **Produktabhängigkeiten**
- Mehr Informationen zu **Produktschwachstellen**
- **Sicherheitskriterien** in Qualitätsprozesse integrierbar
- **Lieferanten** einfacher vergleichbar

Was ändert sich für Anwender?

Forschung & Entwicklung

- Mehr **Transparenz** über eingesetzte Komponenten
- Bessere Übersicht über **Open-Source-Anteile**
- Bekannte **Schwachstellen** schneller erkennbar
- Mehr **Sicherheitsinformationen** für Integrationen
- Weniger **Blackbox-Produkte**

Was ändert sich für Anwender?

Einkauf / Lieferketten

- Mehr **Sicherheitsnachweise** verfügbar
- **Sicherheitsanforderungen** leichter prüfbar
- **Update- und Supportzeiträume** nachvollziehbar
- Mehr Transparenz in der **Lieferkette**
- Cybersicherheit wird **Beschaffungskriterium**

Was ändert sich für Anwender?

Produktentwicklung & -sicherheit

- Mehr Informationen zu **Schwachstellen**
- Mehr Informationen zu **Sicherheitsmaßnahmen**
- **Patchmanagement** besser planbar
- **Risiken** einfacher bewertbar
- **Sicherheitsanforderungen** früher bekannt

Was ändert sich für Anwender?

- Mehr Transparenz über **Abhängigkeiten**
- **Betroffene Systeme** schneller identifizierbar
- **Risikoanalysen** fundierter durchführbar
- **Lieferanten** einfacher bewertbar

Informationssicherheitsverantwortliche

Was sollten Anwender nicht erwarten?

Falsche Erwartungen

- Vollständige Sicherheit
- Haftungsübernahme durch EU
- Fehlerfreie Software
- Ersatz für eigenes Schwachstellenmgmt
- Unterstützung über Produktlebenszyklus hinaus



Sichere Software/Hardware beziehen

hvs consulting

Erfragen

- Wie werden Schwachstellen gemeldet?
- Wie lange werden Updates bereitgestellt?
- Wer ist Sicherheits-Ansprechpartner?
- Gibt es einen Vulnerability-Disclosure-Prozess?

Know-How aufbauen

- CRA-Pflichten verstehen
- Sicherheitsnachweisen bewerten können
- Updatezusagen bewerten
- Schwachstellen-management bewerten
- Beschaffungs-anforderungen definieren

Prüfen

- CRA-Konformitätserklärung
- Technische Dokumentation
- Risikomaßnahmen des Hersteller
- Sichere Standardkonfiguration
- Update- und Supportzeitraum

11. September 2026

11. Dezember 2027

Zusammenfassung

Wer sind Anwender?

Geschäfsleitung, Produktmanagement, Einkauf, Entwicklung, u.v.m.

Neue Garantien

Sichere Standardkonfiguration, Sicherheitsupdates, Herstellerverantwortung, u.v.m

Zusätzliche Informationen

Sicherheitsdokumentation, Produktabhängigkeiten, Sicherheitskontakt, u.v.m

Neue Chancen

Beschaffung, Lieferantenmanagement, Compliance, Schwachstellenmanagement, u.v.m



Vielen Dank!

Paolo Magrini

Georg Janko

BIHK-Reihe zur
IT-Sicherheit, 03.09.2026

hvs consulting

