

Cyber Resilience Act

Ihr Fahrplan zu Compliance und Security bis 2027

dissecto

Sebastian Halbritter – dissecto



- Informatik / OTH
- Automotive Tier1 Umfeld
- 2023 bei dissecto
 - Technologie Entwickler
 - Informationssicherheitsbeauftragter
- Dissecto GmbH
 - gegründet 2022
 - Seit 2016 – Security Forschung
 - EXIST Forschungstransfer
 - Allianz, JLR, FiA, Sony und Kunbus
 - ISO 27001 und TISAX Zerifiziert

1

Don't Believe the Hype

- Der CRA ist kein Marketingtrend.
- Nicht jede Information stimmt.
- Dieses Webinar ist keine Produktwerbung.

- Niemand kennt Ihr Produkt und Ihren Markt besser als Sie!

Warum betrifft der CRA so viele Unternehmen?

- Betrifft alle Produkte mit digitalen Elementen
- Gilt für Hersteller, Importeure und Händler
- Ziel: Sicherere Produkte → mehr Vertrauen im Binnenmarkt
- Konsequenzen bei Verstößen: Bußgelder oder Marktausschluss durch fehlende CE-Kennzeichnung
- Branchen: Maschinenbau | Automotive | IoT | Software
- Regulierung ≠ Norm



Motor Vehicles,
Trailers and
System Regulation
(UN ECE R155)



Medical Devices
Regulation
(MDR)



In Vitro Diagnostic
Medical Devices
Regulation (IVDR)



New Machinery
Directive (EU
Machinery
Regulation)

Vertical

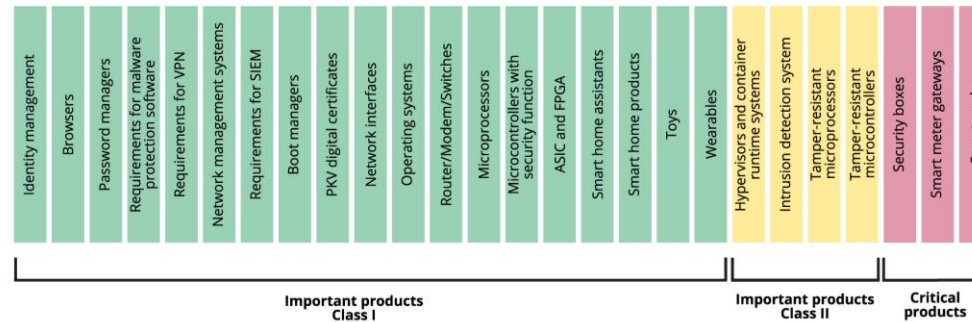
Horizontal

Radio Equipment Directive

Applies to all equipment that uses radio waves for communication or radiodetermination (e.g., Wi-Fi devices, smartphones, infotainment, car key fobs, etc.).

Cyber Resilience Act

Applies to all products with digital elements.



Was fordert der CRA konkret?

- Risikomanagement über den gesamten Lebenszyklus
- Sichere Entwicklungsprozesse (Secure SDLC)
- Patch- & Vulnerability Management
- Vulnerability and Incident Handling & Monitoring
- Dokumentations- und Transparenzpflichten

CRA-Roadmap bis 2027

Jahr	Schwerpunkt	Empfohlene Maßnahmen
2025	Awareness & Gap-Analyse	Zuständigkeiten klären, Risiken erfassen
2026	Umsetzung & Validierung	Prozesse anpassen, Testnachweise automatisieren
2027	Compliance & Audit	Nachweise vorlegen, Marktzugang sichern

Neue Orientierung: prEN 40000-1-1 / -1-2

„ Cybersecurity requirements for products with digital elements“

- Veröffentlicht Oktober 2025
- Erste horizontale Standards zum CRA
- Ziel: Übersetzung regulatorischer Anforderungen in praxisnahe Methodik

- Links:
- prEN 40000-1-1 Vocabulary:
<https://komport.evs.ee/Default.aspx?s=standardCommenting&doc=19689>
- prEN 40000-1-2 Principles for cyber resilience:
<https://komport.evs.ee/Default.aspx?s=standardCommenting&doc=19694>
- Danke, Estland! ;)

Was die prEN 40000 liefert

- Strukturiertes Risikomanagement
- Abdeckung des gesamten Produktlebenszyklus
- Security by Design & Default
- Transparente Kommunikation

Warum das relevant ist

- Verbindet rechtliche Anforderungen mit technischer Praxis
- Liefert Audit-fähige Struktur für Compliance-Nachweise
- Verankert bewährte Best Practices offiziell im CRA-Kontext
- Bietet Orientierung für Hersteller, die bisher ohne konkrete Norm arbeiten mussten

Automotive / Embedded

- Tier-1-Zulieferer aus dem Automotive-Bereich
 - RISS-Umsetzung bereits für OEM-Kunden etabliert
 - Plattform soll auch im Agrarsektor eingesetzt werden
- Gap-Analyse zwischen RISS und CRA, Anpassung der Prozesse

Industrie / IoT-Umfeld

- Hersteller von Industriesensoren ohne bisherige Security-Pflichten
 - Sicherheitsmaßnahmen vorhanden, aber nicht dokumentiert
 - Aufbau einer strukturierten Security-Dokumentation
- Grundlage für ein eigenes Security-Managementsystem

Typische Herausforderungen

- Unklare Verantwortlichkeiten zwischen IT und Entwicklung
- Fehlende Automatisierung bei Security-Tests
- Mangelnde Prozessintegration für Risikomanagement
- Fragmentierte Kommunikation im Unternehmen
- Nachweisführung bei Legacy-Produkten

Legacy Support im CRA

- Risikoüberprüfung auch für Bestandsprodukte
- Updates oder Nachweise erforderlich, solange Produkt vermarktet oder genutzt wird
- Option: Risk Acceptance mit dokumentierter Begründung
- Umgang mit maßgeblichen Änderungen am Produkt

Praxisproblem:

Oft fehlen Dokumentation, Risikoanalysen oder strukturierte Update-Prozesse.

Strategischer Ansatz:

→ Klare Abstimmung zwischen Management & Entwicklung nötig:

- Welche Produkte werden sicherheitsseitig weiter unterstützt?
- Welche werden abgekündigt?
- CRA gilt nur innerhalb der EU – Auslaufprodukte können ggf. außerhalb weiter vertrieben werden.

Langfristige Produkte:

Erfordern dauerhafte Sicherheitsstrategie über Entwicklungs- und Betriebsphase hinweg.

Für Management:

- Rollen, Verantwortlichkeiten und Governance-Struktur klar definieren
- GAP-Analyse gegen CRA + EN 40000
- Security KPIs etablieren

Für Entwicklung / Security:

- Threat Modeling & Risk Assessment standardisieren
- Automatisierte Security-Tests einführen
- Dokumentation digital und revisions sicher führen

Der Fahrplan zur CRA-Compliance

1. 2025: Bewusstsein & Risikobewertung
2. 2026: Implementierung gemäß EN 40000
3. 2027: Audit & Nachweisführung → Automatisierung + klare Prozesse
= Sichere Marktzulassung

- CRA = Verpflichtung + Chance
- EN 40000 schafft endlich Handlungsrahmen
- Wer jetzt beginnt, sichert Marktzugang und Wettbewerbsvorteil

Danke für die Aufmerksamkeit

Fragen?