CRA-READINESS · QUICK-CHECK

Sind Sie für den Cyber Resilience Act bereit?

Fünf Kernfragen, drei nächste Schritte. Kostenfrei und ohne Anmeldung.

Wann der CRA Sie trifft

Der Cyber Resilience Act ist seit dem 10. Dezember 2024 in Kraft. Meldepflichten greifen ab 11. September 2026. Volle Konformität bis 11. Dezember 2027. Bußgeld-Risiko: bis zu 15 Mio. € oder 2,5 % des weltweiten Jahresumsatzes.

PSIRT as a Service

Marcel Schick · m.schick@rait.systems · +49 152 24531405

Securist ist eine Marke der RAIT Systems GmbH · Brunnenstraße 15 · 88480 Achstetten

DER QUICK-CHECK

Fünf Kernfragen zum CRA-Stand

Beantworten Sie jede Frage ehrlich. Eine ehrliche „Nein“-Antwort ist kein Misserfolg — sie ist die Voraussetzung dafür, dass Sie einen Plan bauen können.

CRA-Pflicht	Ja	Teilweise	Nein	Unsicher
1. PSIRT-Kontaktstelle. Wir haben eine öffentliche Anlaufstelle für Schwachstellenmeldungen (Telefon, Web-Formular oder E-Mail) mit definierter Reaktionszeit unter 24 Stunden.	■	■	■	■
2. Schwachstellen-Bewertung. Wir können eingehende CVEs technisch bewerten, CVSS-Scores vergeben und Impact-Einstufungen für unsere Produkte vornehmen.	■	■	■	■
3. Behördenmeldung in 24h / 72h. Wir haben einen dokumentierten Prozess, um aktiv ausgenutzte Schwachstellen binnen 24 Stunden an ENISA zu melden und einen Bericht binnen 14 Tagen zu liefern.	■	■	■	■
4. Security Advisories. Wir veröffentlichen Security Advisories an unsere Kunden mit klarer Schwachstellen-Beschreibung, Workaround und Patch-Information.	■	■	■	■
5. Dokumentation für Audits. Alle Schwachstellen-Meldungen, Bewertungen, Maßnahmen und Lessons Learned sind lückenlos und auditfähig dokumentiert.	■	■	■	■

Was diese Tabelle nicht zeigt

Die einzelnen Pflichten wirken überschaubar — kumuliert wird es anspruchsvoll. Wie anspruchsvoll, hängt stark von Ihrem Setup ab: schlankes Produktportfolio und vorhandene IT-Security-Struktur kommen oft mit **1–2 FTE plus 24/7-Bereitschaft** aus. Mehrere Produktlinien, OT/ICS oder internationale Auslieferung — dann landen Hersteller typischerweise bei **vier bis fünf Vollzeitkräften und 300.000 bis 600.000 € pro Jahr**. Plus Recruiting, Tooling und Schulung. Die ehrliche Frage ist nicht „wie viele Manntage“, sondern „wie sieht es bei uns konkret aus“.

AUSWERTUNG

Was Ihr Ergebnis bedeutet

5× Ja · CRA-ready

Glückwunsch. Sie haben die Substanz, brauchen aber wahrscheinlich Hilfe bei der Skalierung — Audits, mehr Produktlinien, internationale Behördenkommunikation.

3–4× Ja · Solide Grundlage, Lücken vorhanden

Sie haben Strukturen, aber ein PSIRT-Service kann gezielt die teuersten 1–2 Lücken schließen — typischerweise CVE-Bewertung oder ENISA-Meldekommunikation.

0–2× Ja · Akuter Handlungsbedarf

Sie sind unter Zugzwang. Ab September 2026 greifen Meldepflichten, ab Dezember 2027 volle Konformität. Ein PSIRT-Aufbau (intern oder als Service) sollte in den nächsten 60 Tagen entschieden sein.

DREI NÄCHSTE SCHRITTE

Was jetzt sinnvoll ist

1. Stand intern dokumentieren

Notieren Sie Ihre fünf Antworten und teilen Sie sie mit Geschäftsführung oder CISO. Allein dieser Schritt verschafft Klarheit über den realen Reifegrad.

2. Vollversion der Checkliste anfordern

Die ausführliche Version mit 12 Pflichten, detaillierter Aufwandsrechnung und Self-Assessment-Score gibt es nach kurzer Anmeldung auf security-done-right.de.

3. 30-Minuten-Discovery-Call

Wir gehen Ihre Antworten gemeinsam durch und klären, ob ein BASIC-, PRO- oder ENTERPRISE-Bundle passt — oder ob ein interner Aufbau sinnvoller ist. Ohne Verkaufsdruck.

Lust auf den nächsten Schritt?

Buchen Sie ein 30-Minuten-Discovery-Gespräch oder laden Sie die Vollversion der CRA-Readiness-Checkliste herunter — mit allen 12 Pflichten, Score-System und Build-vs-Buy-Rechnung.

→ **security-done-right.de/kontakt**