CYBER RESILIENCE ACT

CRA-Meldepflichten

Checkliste für Hersteller von Produkten mit digitalen Elementen

Stichtag 11. September 2026 · 7 Themenbereiche · 25 Checkpoints

1 Schwachstellenmanagement-Prozess etablieren

Ziel: Sicherheitslücken in eigenen Produkten systematisch erkennen, bewerten und schließen, bevor andere sie ausnutzen.

- [ ] **1.1 SBOM erstellen**

  Vollständige Liste aller Softwarekomponenten und Abhängigkeiten mit Versionsnummer für alle betroffenen Produkte. Ohne SBOM kein effektives Vulnerability Monitoring, und keine CRA-Compliance.

- [ ] **1.2 Automatisiertes Schwachstellen-Scanning einrichten**

  SBOM automatisiert gegen CVE-Datenbanken abgleichen (NVD, ENISA European Vulnerability Database). Open-Source-Einstieg: OWASP Dependency-Track oder Trivy. Scan-Ergebnisse müssen ins Ticket-System fließen.

- [ ] **1.3 CVSS-Bewertungskompetenz sicherstellen**

  Mindestens eine Person im Team muss CVSS v3.1/v4.0 korrekt anwenden können. CVSS-Score allein reicht nicht, Ausnutzbarkeit im eigenen Produktkontext muss beurteilt werden.

- [ ] **1.4 Triage-Prozess für eingehende Schwachstellenmeldungen definieren**

  Wer prüft neue CVEs, in welchem Zeitfenster, mit welchen Schwellenwerten? Beispiel-SLA: CVSS ≥ 9.0 + bekannte Ausnutzung → PSIRT-Aktivierung innerhalb von 2 Stunden.

- [ ] **1.5 Patch-Prozess und Updateverteilung dokumentieren**

  Wie werden Sicherheits-Updates erstellt, getestet und an Nutzer verteilt? Für eingebettete Systeme: OTA-Update-Fähigkeit prüfen. Ohne funktionierende Update-Kette kein Abschlussbericht möglich.

2 Meldekanal für Sicherheitsforscher einrichten (CVD-Policy)

Ziel: Externe Sicherheitsforscher haben einen klaren, öffentlich zugänglichen Weg, Schwachstellen verantwortungsvoll zu melden, bevor sie öffentlich werden oder ausgenutzt werden.

- [ ] **2.1 security.txt-Datei und Meldeseite einrichten**

  Erreichbar unter security.txt (RFC 9116) auf der eigenen Domain. Enthält: Kontaktadresse, PGP-Key (empfohlen), Scope, Sprache, bevorzugtes Format. Ohne diesen Kanal keine CRA-Compliance.

- [ ] **2.2 CVD-Policy verabschieden und veröffentlichen**

  Dokument mit Scope, Umgang mit Forschern, Fristen (üblich: 45 bis 90 Tage bis Veröffentlichung), Schutz vor Strafverfolgung bei verantwortungsvoller Meldung. Referenz: ENISA-Leitlinien oder ISO/IEC 29147.

2.3 Internen Eingang für Forschermeldungen aufbauen

Wer empfängt, wer bestätigt den Eingang binnen 3 Werktagen, wer bewertet, wer kommuniziert? Dedizierte E-Mail-Adresse (psirt@[unternehmen].de) ist Mindeststandard. CVD-Meldung und CRA-Pflichtmeldung sind getrennte Prozesse.

3 PSIRT aufbauen

Product Security Incident Response Team

Ziel: Eine definierte, einsatzbereite Gruppe, die im Ernstfall sofort handlungsfähig ist, nicht erst zusammengesucht werden muss.

3.1 PSIRT-Rollen benennen und schriftlich fixieren

Vier Pflicht-Rollen: (1) PSIRT Lead, Gesamtverantwortung, (2) Technical Lead, Schwachstellenanalyse, (3) Legal/Compliance Liaison, Meldepflichten, (4) Communications Manager, externe Kommunikation inkl. ENISA-Meldung. Stellvertreterregelung für alle Rollen. Für KMU reicht oft eine gut ausgebildete Person mit klaren Prozessen.

3.2 24/7-Erreichbarkeit sicherstellen

Wer kann zu welcher Zeit eine CRA-Meldung autorisieren und absenden? Rufbereitschaftsplan dokumentieren. Die 24-Stunden-Frist läuft auch am Sonntagabend und an Feiertagen.

3.3 PSIRT-Kommunikationskanal einrichten

Dedizierter Kanal (verschlüsselter Workspace oder gesonderter Teams-Kanal) für den Ernstfall, schneller und sicherer als ein E-Mail-Verteiler unter Zeitdruck.

4 Meldezugang zur ENISA Single Reporting Platform (SRP) einrichten

Ziel: Im Ernstfall sofort melden können, nicht erst Zugangsdaten suchen.

4.1 Hauptniederlassung in der EU bestimmen

Der Meldeweg richtet sich nach dem Sitz der Hauptniederlassung in der EU. Das legt fest, welches nationale CSIRT zuständig ist und an welches CSIRT die SRP-Meldung adressiert wird.

4.2 ENISA SRP-Registrierung vorbereiten

ENISA hat angekündigt, dass die SRP ab dem 11. September 2026 für Pflichtmeldungen genutzt wird. Factsheet, FAQ und Anleitungen für die Registrierung liegen vor, zuletzt aktualisiert im August 2026. Die Registrierung läuft über EU Login, mit einem primären und einem sekundären Vertreter. Eine Schnittstelle zur automatisierten Übermittlung ist zunächst nicht vorgesehen, gemeldet wird im Browser. Wer eine vollautomatische Meldekette plant, plant an der Realität vorbei.

4.3 Backup-Meldeweg dokumentieren

Falls die SRP im Ernstfall nicht erreichbar ist: direkter Kontakt zum nationalen CSIRT. Für Deutschland zuständig ist CERT-Bund beim BSI (cert@bsi.bund.de). Die gesetzliche Grundlage dafür liegt als Regierungsentwurf vor, der dem BSIG einen entsprechenden Aufgabenzusatz einfügt. Faktisch ist die Zuständigkeit klar, formal war sie im September 2026 noch nicht abgeschlossen.

4.4 Melde-Templates vorab erstellen und freigeben

Vorausgefüllte Templates für Frühwarnung (24 h) und Vollmeldung (72 h) mit allen Pflichtfeldern. Leer-Felder klar kennzeichnen. Templates durch Legal Liaison und Technical Lead freigeben lassen, bevor sie gebraucht werden.

5 Interne Eskalationsmatrix definieren

Ziel: Von der ersten Warnung bis zur ENISA-Meldung gibt es für jeden Schritt einen Verantwortlichen, eine Frist und einen Eskalationsweg.

5.1 Erkennungsquellen und Trigger definieren

Welche Signale lösen den PSIRT-Prozess aus? Mindestens: (a) CVSS-kritische CVE in SBOM-Komponente, (b) externe Forschermeldung via CVD-Kanal, (c) SIEM-Alert, (d) Kundenmeldung mit Exploit-Beschreibung, (e) öffentliche PoC-Veröffentlichung.

5.2 Schweregrad-Klassifizierung intern vereinbaren

Zwei CRA-Kategorien: (A) Aktiv ausgenutzte Schwachstelle → 24-Stunden-Meldepflicht. (B) Schwerer Sicherheitsvorfall → gesonderter Meldeprozess. Interne Kriterien schriftlich fixieren, damit im Ernstfall kein Interpretationsstreit entsteht.

5.3 Eskalationsmatrix auf einer Seite dokumentieren

Wer wird bei welchem Trigger sofort informiert? Wer entscheidet innerhalb welcher Zeit über den Schweregrad? Wer autorisiert die ENISA-Meldung? Wer kommuniziert an Kunden? Format: Tabelle oder Flussdiagramm, ausdruckbar.

5.4 Schnittstellen zu anderen Meldepflichten kartieren

NIS2 (falls anwendbar) und DSGVO (bei personenbezogenen Daten) können parallel greifen. Parallelität dokumentieren, Doppelmeldung vermeiden, Widersprüche rechtlich klären.

6 Notfallplan für aktiv ausgenutzte Schwachstellen

Playbook

Ziel: Im Ernstfall nicht überlegen, was zu tun ist, sondern abarbeiten.

6.1 Incident Response Playbook für CRA-Vorfälle erstellen

Konkreter Ablaufplan: Trigger → PSIRT-Aktivierung → Schweregradbewertung → Meldung → Patch → Kundenkommunikation → Abschluss. Maximal vier Seiten, kein Fachjargon.

6.2 Entscheidungsbaum für Meldepflicht-Auslösung erstellen

Kernfrage: „Gibt es verlässliche Nachweise für aktive Ausnutzung?" Wenn ja → 24-Stunden-Frist läuft. Wenn nein → CVD-Prozess, keine CRA-Pflichtmeldung. Muss im Stressmoment in unter 5 Minuten anwendbar sein.

6.3 Erste-Hilfe-Karte für den Ernstfall laminieren

Einseitig, klar strukturiert: Wer ruft wen an, wer entscheidet, welche Nummer hat das BSI CERT-Bund, wo ist das Melde-Template, wie lautet die SRP-URL. Neben dem Bildschirm oder in der Notfallmappe.

7 Probelauf durchführen und dokumentieren

Ziel: Den Prozess vor dem Ernstfall geprobt haben, nicht zum ersten Mal unter Zeitdruck.

7.1 Tabletop-Exercise zum CRA-Szenario durchführen

Simuliertes Szenario: „Ein Sicherheitsforscher meldet, dass eine Komponente in Produkt X aktiv ausgenutzt wird. Es ist Freitagabend 18:30 Uhr." Alle PSIRT-Rollen durchspielen. Schwachstellen im Prozess identifizieren und nachbessern.

7.2 Meldeprozess auf dem SRP-Testsystem erproben

Sobald die ENISA-Testumgebung verfügbar ist (geplant vor September 2026): vollständigen Meldeprozess einmal durchlaufen. Technische Hürden vor dem Ernstfall kennen.

7.3 Nachweis der Übung dokumentieren

Datum, Teilnehmer, Szenario, Erkenntnisse, Maßnahmen festhalten, für zukünftige Behördenanfragen. Marktüberwachungsbehörden können nach der Prozessdokumentation fragen.

> **Frist-Erinnerung**
>
> Der 11. September 2026 ist ein harter Termin. Der Aufbau dieser Strukturen dauert realistisch vier bis fünf Monate, wenn man bei null startet. Die 24-Stunden-Frist läuft auch an Wochenenden und Feiertagen.

Quelle und Rechtsgrundlage: CRA Art. 14 (Meldepflichten) und Art. 16 (Single Reporting Platform), Verordnung (EU) 2024/2847. Bußgeldrahmen bei Nichtmeldung: bis 15 Mio. € oder 2,5 % des globalen Jahresumsatzes (Art. 64). Diese Checkliste ist eine Orientierungshilfe und ersetzt keine Rechtsberatung. Eigene Darstellung. Stand: September 2026