IT-BERATER / ARBEITSHILFEN

Cyber Resilience Act Organisationspaket

Organisatorische CRA-Arbeitshilfe und Belegsammlung.

Arbeitsmappe · Bearbeitbare Ausgabe

Abbildung 1 · Titelmotiv; ergänzende Illustration. Maßgeblich sind Leitfaden und ausgefüllte Karten.

Dateien öffnen

Entpacken Sie das vollständige ZIP zuerst in einen eigenen Ordner. Öffnen Sie im Hauptordner `produktsicherheit-guide-de.pdf` als Leitfaden und `produktsicherheit-workbook-de.pdf` als separate Arbeitsmappe. Die gleichnamigen DOCX-Dateien sind bearbeitbar. `produktsicherheit-full-de.pdf` enthält zusätzlich alle Beispiele, Übungen, Quellen und Lizenzinformationen zusammen in einem Dokument. Weitere bearbeitbare Vorlagen liegen unter `editable/de/`; Markdown- und CSV-Arbeitsdateien unter `package/de/`. Die englische Fassung ist ebenfalls enthalten.

Deutschland/EU · Stand 19.09.2026 · 79 EUR

Ergebnis: eine nachvollziehbare Fallakte mit belegten Antworten, benannten offenen Fragen und klarer Übergabe.

• GUIDE_DE.md lesen und Rollen/Belegablage festlegen.

• WORKBOOK_DE.csv als UTF-8 importieren oder die Markdown-Vorlage kopieren. Pro Vorgang eigene Datei verwenden.

• Mit den vollständig ausgefüllten Faellen A/B ueben; diese verwenden ausschließlich fiktive Belege.

• Reale Antworten mit Beleg, Owner, Datum, nächster Aktion und Review erfassen. Unbekanntes bleibt offen; nicht anwendbar braucht eine Begründung.

• Vor Abschluss die Umsetzung und erreichbare Nachweise prüfen.

INVENTORY_DE.md nennt jede enthaltene Datei; LICENSE_DE.md beschreibt die interne Nutzung. SOURCES.md dokumentiert die Rechtsquellen. Die Arbeitshilfe ersetzt keine konkrete Fachentscheidung oder Rechtsberatung. Die englische Fassung erweitert den Geltungsbereich nicht.

Leitfaden: CRA-Readiness als Organisationsroutine

Zweck und Grenzen

Der Cyber Resilience Act (CRA) wird hier als Arbeitsablauf behandelt: Produktbestand erfassen, Rolle und Geltungsbereich prüfen, Cyberrisiko dokumentieren, Secure-by-Design-Nachweise sammeln, Schwachstellenkanal betreiben, Supportperiode festlegen und Vorfälle eskalieren. Der Leitfaden ist keine Konformitätsbewertung, kein Audit und keine Rechtsberatung.

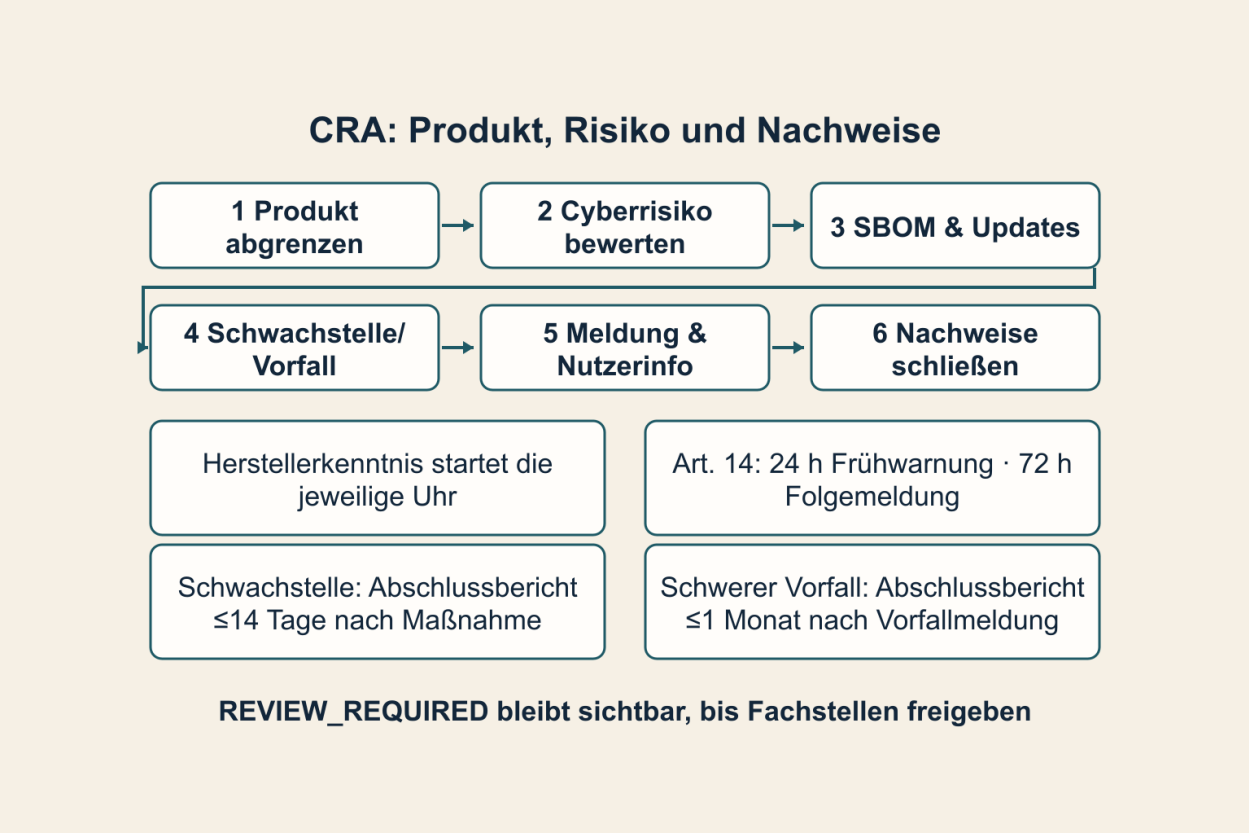

Abbildung 2 · Arbeitsablauf; ergänzende Illustration. Maßgeblich sind Leitfaden und ausgefüllte Karten.

1. Produkt und Rolle abgrenzen

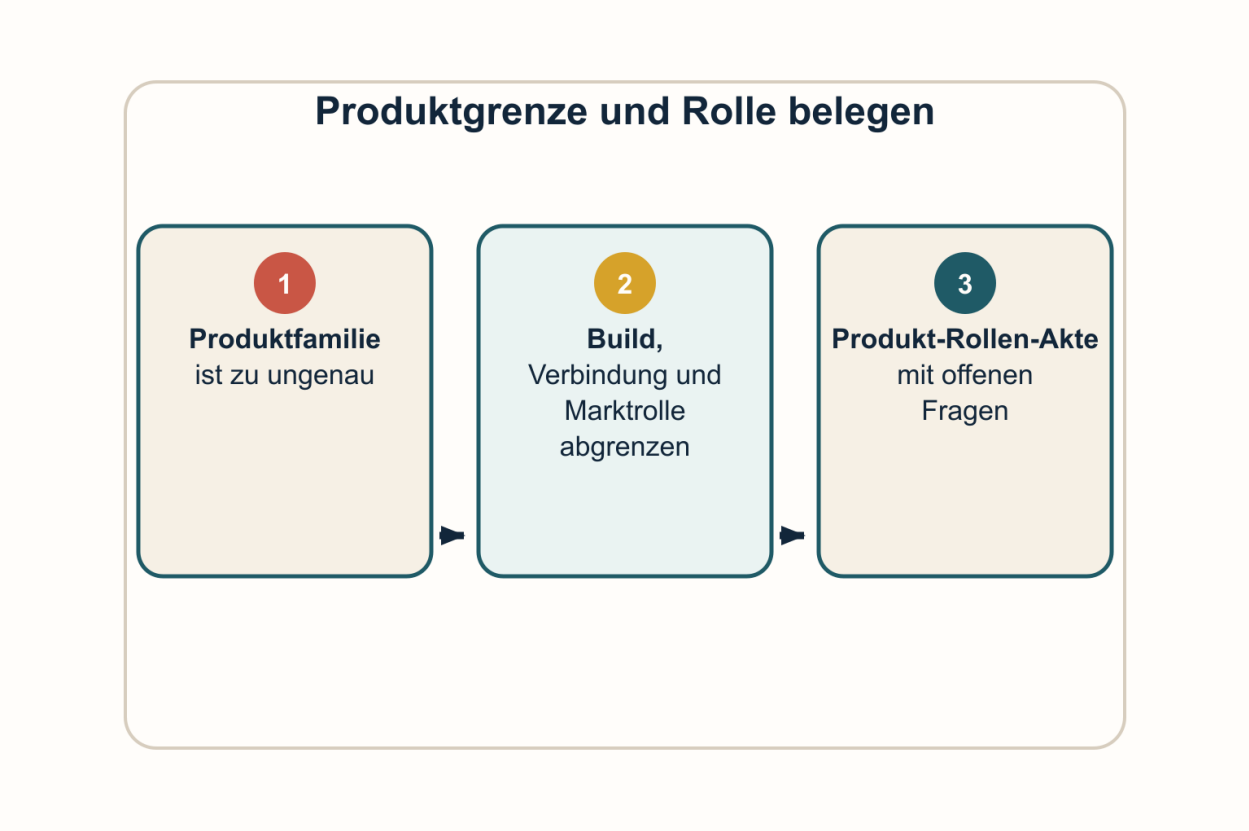

Abbildung 3 · Produktgrenze und Rolle belegen. Situation, Handlung und begrenztes Ergebnis.

Erfasse Produktname, Version, Varianten, Hersteller, Importeur, Distributor, Open-Source-Steward, EU-Markt und Daten-/Netzverbindung. CRA Art. 2 knüpft an Produkte mit digitalen Elementen an, deren bestimmungsgemäße oder vernünftigerweise vorhersehbare Nutzung eine direkte oder indirekte Verbindung umfasst. Prüfe Ausschlüsse und Überschneidungen, etwa sektorale Rechtsakte, in `M7-CRA-01`; ein „scope likely“ ist kein Rechtsurteil.

2. Risiko und sichere Entwicklung

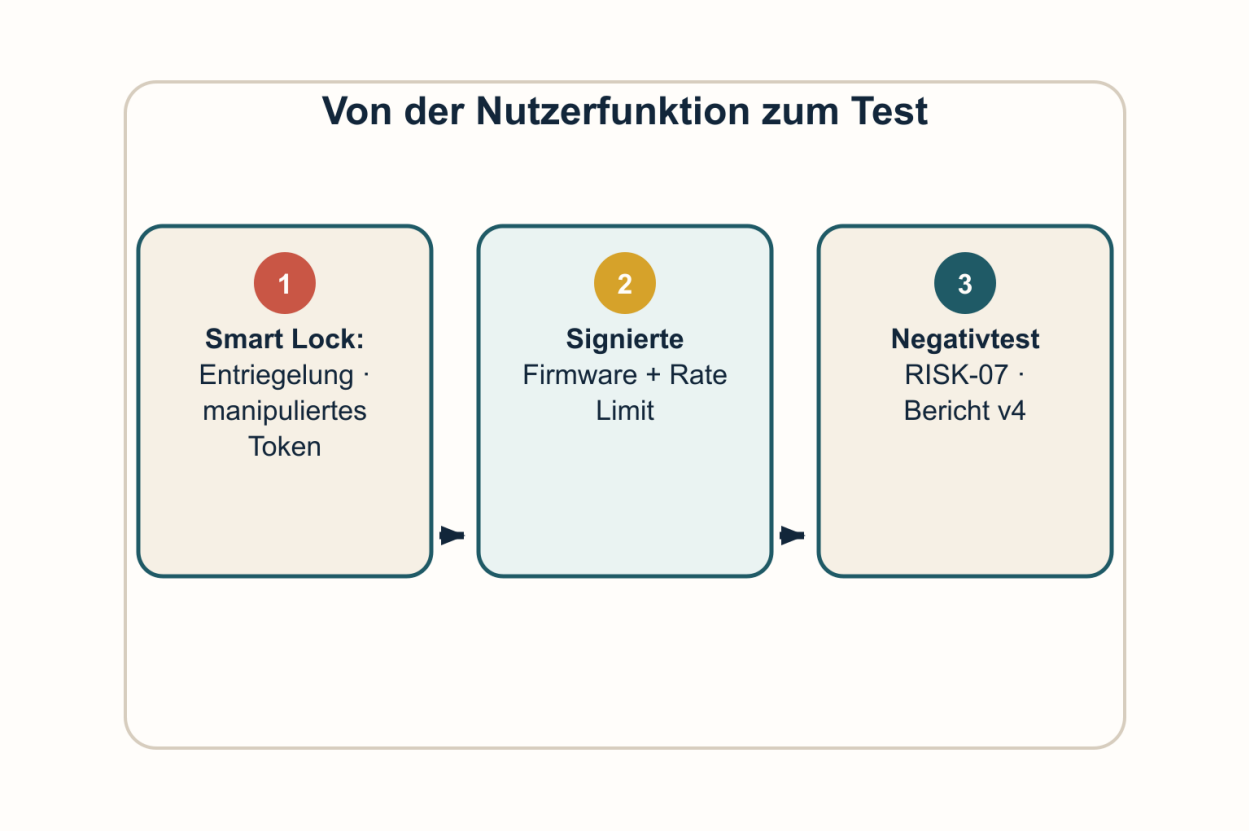

Abbildung 4 · Von der Nutzerfunktion zum Test. Situation, Handlung und begrenztes Ergebnis.

Nach Art. 13 dokumentiert der Hersteller eine Cyberrisikobewertung und berücksichtigt sie in Planung, Entwicklung, Produktion, Lieferung und Wartung. Erfasse Schutzgüter, Angriffsflächen, Annahmen, Betriebsumgebung, erwartete Nutzungsdauer, Restrisiko, Maßnahmen und offene Entscheidungen. Annex I Part I nennt unter anderem bekannte ausnutzbare Schwachstellen, sichere Standardkonfiguration, Updates, Zugriffskontrolle, Vertraulichkeit, Integrität, Verfügbarkeit und Datenminimierung.

3. Komponenten und SBOM

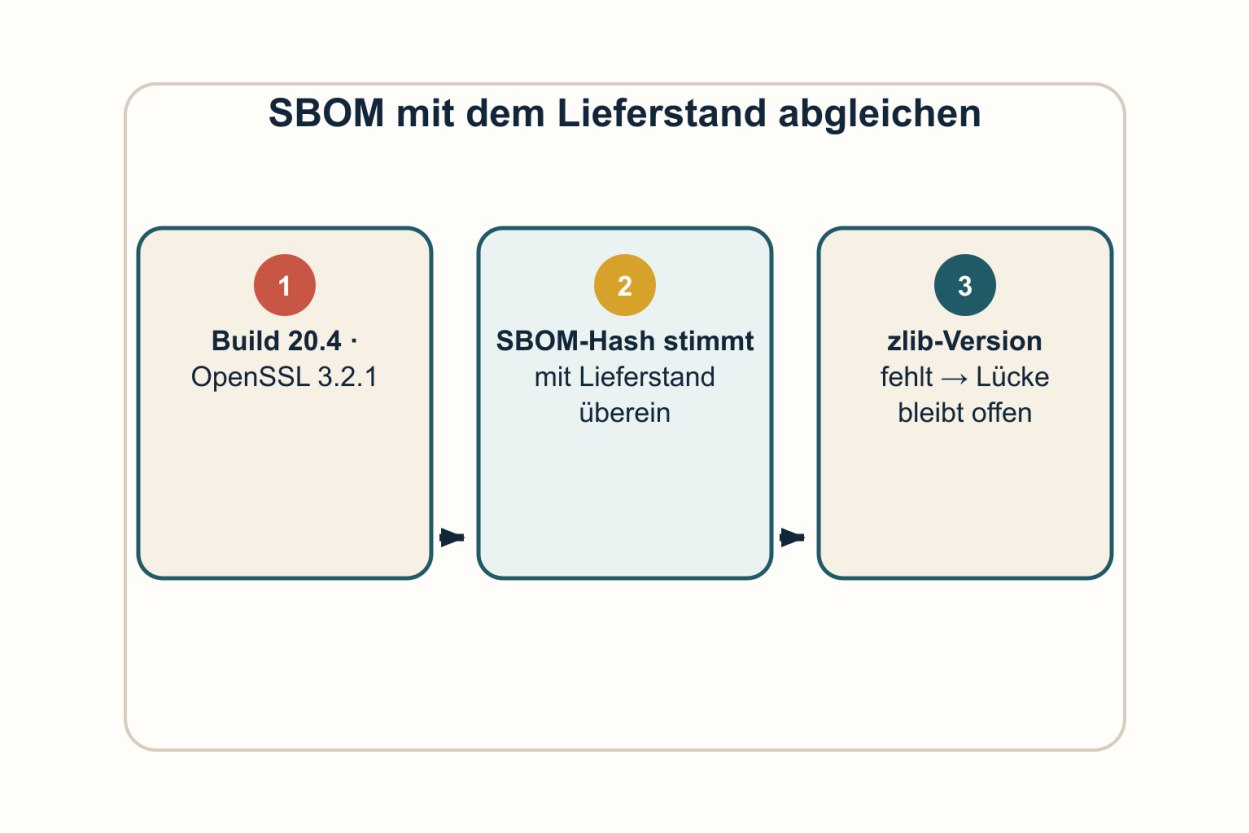

Abbildung 5 · SBOM mit dem Lieferstand abgleichen. Situation, Handlung und begrenztes Ergebnis.

Erstelle eine verifizierbare Komponentenliste/SBOM mit Version, Herkunft, Lizenz, Verantwortlichem und Prüfnachweis. CRA Annex I Part II verlangt mindestens Top-Level-Abhängigkeiten in einem gängigen maschinenlesbaren Format. Das Workbook dokumentiert Status, nicht die technische Richtigkeit der SBOM.

4. Vulnerability Handling

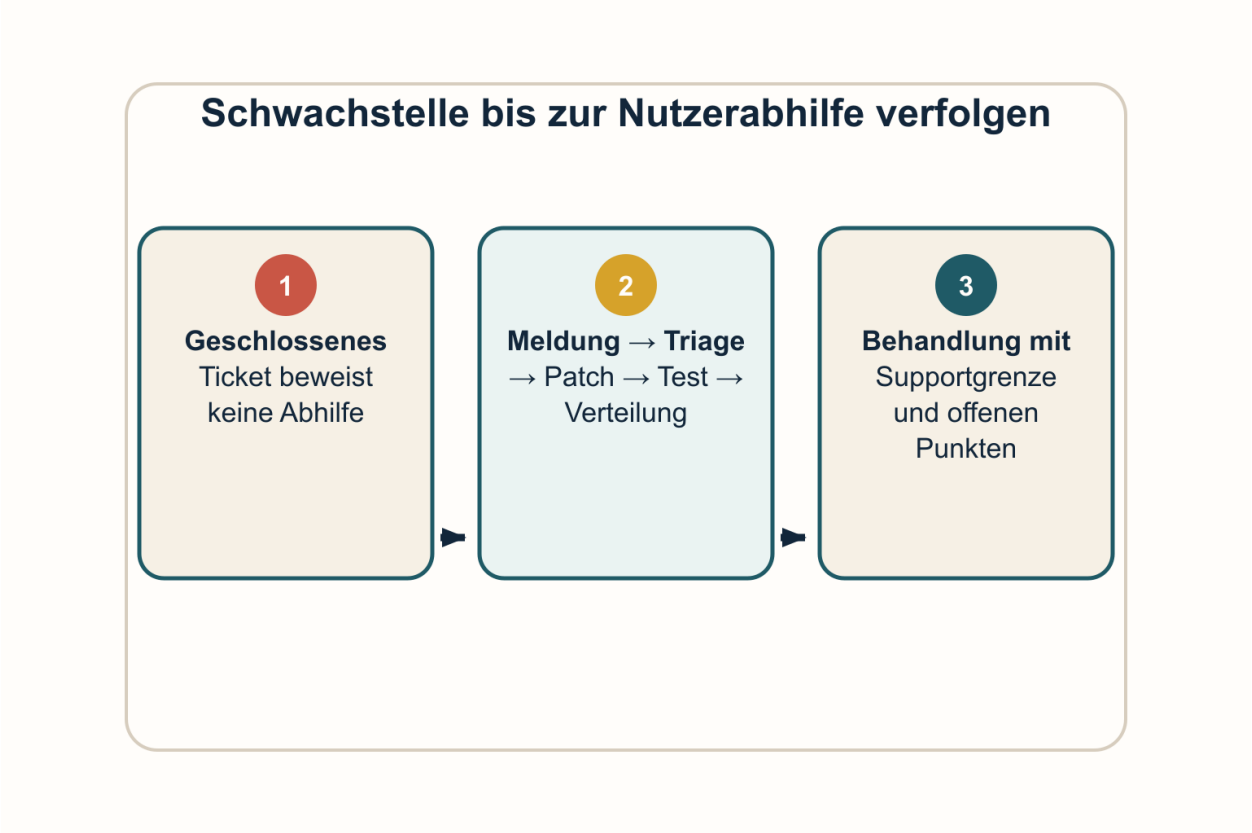

Abbildung 6 · Schwachstelle bis zur Nutzerabhilfe verfolgen. Situation, Handlung und begrenztes Ergebnis.

Richte einen veröffentlichten Meldekontakt, Triage, Schweregrad, Verantwortlichen, Patch-/Mitigation-Entscheidung, Test, sichere Verteilung und Disclosure-Nachweis ein. Dokumentiere, ob Updates getrennt von Funktionsupdates bereitgestellt werden können. Definiere Supportperiode und Supportende nachvollziehbar; Art. 13 nennt grundsätzlich mindestens fünf Jahre, wenn die erwartete Nutzungsdauer nicht kürzer ist. Kein Feld darf als „sicher“ markiert werden, wenn nur eine Selbstauskunft vorliegt.