CRA-Checkliste zu Anhang I, Art. 13 und Art. 14

Hinweis
Eine Zeile je Anforderung, zu bewerten je Produkt und Produktversion. Tragen Sie den Status (offen / teilweise / erfüllt / nicht anwendbar), Ihren Nachweis aus der technischen Dokumentation, die verantwortliche Person und einen Termin ein. Nicht anwendbare Anforderungen begründen Sie in der Risikobewertung.

Anhang I – Grundlegende Cybersicherheitsanforderungen

Teil I – Anforderungen an die Eigenschaften von Produkten mit digitalen Elementen

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
1	Angemessenes Cybersicherheitsniveau angesichts der Risiken Anhang I Teil I Nr. 1	Nachweis über die Risikobewertung (Art. 13 Abs. 2, 3) und einen dokumentierten sicheren Entwicklungsprozess (z. B. nach IEC 62443-4-1): Security-Anforderungen, Threat Modeling, sichere Codierung, Reviews, Tests. Die Risikobewertung muss angeben, wie Nr. 1 angewendet wird.		
2	Bereitstellung ohne bekannte ausnutzbare Schwachstellen Anhang I Teil I Nr. 2 Buchst. a	Release-Gate mit SBOM-Abgleich gegen Schwachstellendatenbanken; Bewertung der Ausnutzbarkeit je Fund (VEX); Prüfung von Lagerware vor Auslieferung. Nachweis: Scan-Berichte und Freigabeprotokoll je Release.		
3	Sichere Standardkonfiguration und Rücksetzbarkeit Anhang I Teil I Nr. 2 Buchst. b	Tabelle der Standardkonfiguration (Dienste, Ports, Konten, Standardzustand) und Nachweis, dass keine Standardpasswörter existieren; Test des Werksresets. Abweichungen für maßgeschneiderte Produkte vertraglich dokumentieren.		
4	Behebung von Schwachstellen durch Sicherheitsaktualisierungen Anhang I Teil I Nr. 2 Buchst. c	Update-Mechanismus mit Signaturprüfung; Entscheidung zu automatischen Updates (inkl. Opt-out, Benachrichtigung, Aufschieben) in der Risikobewertung begründen. Nachweis: Update-Konzept und Testbericht zum Update-Pfad.		
5	Schutz vor unbefugtem Zugriff und Meldung möglicher unbefugter Zugriffe Anhang I Teil I Nr. 2 Buchst. d	Rollen- und Rechtekonzept, Authentifizierung (lokal/zentral), Brute-Force-Schutz, Protokollierung fehlgeschlagener Anmeldungen. Nachweis: Designdokument, Pentest-Bericht zu Authentifizierung und Autorisierung.		
6	Vertraulichkeit gespeicherter, übermittelter und verarbeiteter Daten Anhang I Teil I Nr. 2 Buchst. e	Verschlüsselung nach Stand der Technik (z. B. TLS 1.2/1.3, verschlüsselte Speicherung von Zugangsdaten und Rezepturen), Schlüsselspeicherung in Hardware. Nachweis: Kryptokonzept mit Verweis auf BSI TR-02102, Konfigurationsprüfung.		
7	Integrität von Daten, Befehlen, Programmen und Konfigurationen; Meldung von Beschädigungen Anhang I Teil I Nr. 2 Buchst. f	Secure Boot, signierte Firmware und Anwendungsprogramme, Integritätsprüfung von Konfigurationen, Erkennung und Meldung von Manipulationen. Nachweis: Test mit manipuliertem Image, Protokoll der Ablehnung.		

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
8	Datenminimierung Anhang I Teil I Nr. 2 Buchst. g	Datenverzeichnis: welche (personenbezogenen und sonstigen) Daten, wozu, wohin. Telemetrie nur im erforderlichen Umfang und konfigurierbar. Nachweis: Datenflussanalyse und Konfigurationsoptionen.		
9	Verfügbarkeit wesentlicher und grundlegender Funktionen, auch nach Vorfällen und bei DoS Anhang I Teil I Nr. 2 Buchst. h	Definition der wesentlichen Funktionen; Rate Limiting, Priorisierung des Echtzeitverkehrs, sicherer Zustand bei Überlast. Nachweis: Robustheits- und Lasttestberichte (z. B. Netzwerk-Stresstests, Fuzzing).		
10	Minimierung negativer Auswirkungen auf andere Geräte und Netze Anhang I Teil I Nr. 2 Buchst. i	Begrenzung von Broadcast/Multicast und Wiederverbindungsversuchen, keine ungefilterte Brückenfunktion zwischen Netzen, Fernwartung nur kontrolliert. Nachweis: Architekturbewertung und Netzwerktests.		
11	Begrenzung der Angriffsflächen, auch bei externen Schnittstellen Anhang I Teil I Nr. 2 Buchst. j	Schnittstelleninventar mit Begründung jeder offenen Schnittstelle; Debug-Schnittstellen (JTAG/UART) in Serie deaktiviert oder geschützt; minimales OS-Image. Nachweis: Port-Scan, Hardware-Review.		
12	Verringerung der Auswirkungen von Vorfällen durch Mechanismen gegen Ausnutzung Anhang I Teil I Nr. 2 Buchst. k	Compiler-Härtung (Stack-Schutz, ASLR, NX), Least Privilege für Prozesse, Sandboxing, Trennung sicherheitskritischer Funktionen. Nachweis: Build-Konfiguration, Härtungscheck (z. B. checksec).		
13	Sicherheitsbezogene Protokollierung/Überwachung mit Opt-out Anhang I Teil I Nr. 2 Buchst. l	Security-Log für Anmeldungen, Konfigurations-, Programm- und Firmwareänderungen; Export (Syslog); Opt-out-Möglichkeit dokumentieren. Nachweis: Log-Konzept und Beispielprotokolle.		
14	Dauerhaftes sicheres Löschen und sichere Übertragung von Daten und Einstellungen Anhang I Teil I Nr. 2 Buchst. m	Werksreset bzw. Löschfunktion für alle Daten, Konten, Zertifikate und Schlüssel; sichere Export-/Importfunktion für Konfigurationen. Nachweis: forensischer Löschtest, Anleitung in den Nutzerinformationen (Anhang II Nr. 8 Buchst. d).		

Teil II – Anforderungen an die Behandlung von Schwachstellen

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
15	Schwachstellen und Komponenten ermitteln und dokumentieren, Software-Stückliste Anhang I Teil II Nr. 1	SBOM in maschinenlesbarem Format (CycloneDX/SPDX) mit mindestens den obersten Abhängigkeiten je Release; kontinuierliches Monitoring. Nachweis: SBOM-Konzept, SBOM-Register, Monitoring-Protokolle.		
16	Schwachstellen unverzüglich behandeln und beheben; Sicherheitsupdates getrennt von Funktionsupdates Anhang I Teil II Nr. 2	Dokumentierter PSIRT-Prozess mit Reaktionszielen, Wartungszweigen und eigenständigen Sicherheitsupdates. Nachweis: Verfahrensanweisung, Ticket-Historie mit Zeitstempeln.		
17	Regelmäßige und wirksame Sicherheitstests und -überprüfungen Anhang I Teil II Nr. 3	Testplan mit SAST, Abhängigkeits-Scans, Fuzzing, Pentests und Turnus. Nachweis: Testberichte in der technischen Dokumentation (Anhang VII Nr. 6).		

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
18	Informationen über behobene Schwachstellen veröffentlichen Anhang I Teil II Nr. 4	Security Advisories (z. B. CSAF 2.0) mit Beschreibung, betroffenen Produkten/Versionen, Auswirkung, Schweregrad und Abhilfe; Kriterien für begründetes Aufschieben. Nachweis: veröffentlichte Advisories, Freigabeprozess.		
19	Strategie für die koordinierte Offenlegung von Schwachstellen (CVD) Anhang I Teil II Nr. 5	Öffentliche CVD-Policy mit Meldeweg, Zusagen, Zeitrahmen und Safe Harbor. Nachweis: veröffentlichte Policy (Screenshot/URL), Verweis in den Nutzerinformationen (Anhang II Nr. 2).		
20	Informationsaustausch über Schwachstellen erleichtern, Kontaktadresse angeben Anhang I Teil II Nr. 6	Funktionspostfach mit PGP, Webformular, security.txt; Kanäle zu Lieferanten und Koordinationsstellen (z. B. CERT@VDE). Nachweis: Kontaktangaben auf Website und in der Produktdokumentation.		
21	Mechanismen für die sichere Verbreitung von Aktualisierungen Anhang I Teil II Nr. 7	Signierte Pakete, authentifizierter Download-Kanal, Integritätsprüfung vor Installation, ggf. automatische Verteilung; Offline-Pfad für abgeschottete Anlagen. Nachweis: Update-Konzept und Test der Signaturprüfung.		
22	Sicherheitsupdates unverzüglich und kostenlos mit Hinweisen verbreiten Anhang I Teil II Nr. 8	Regelung zur Kostenfreiheit (Ausnahmen nur vertraglich bei maßgeschneiderten Produkten für gewerbliche Nutzer); Release Notes mit Handlungsempfehlungen. Nachweis: Update-Richtlinie, Beispiel-Release-Notes.		

Pflichten der Hersteller und Meldepflichten (Art. 13 und 14)

Pflichten der Hersteller (Art. 13)

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
23	Cybersicherheitsrisiken bewerten, dokumentieren und aktuell halten Art. 13 Abs. 2, 3, 4 und 7	Die Risikobewertung begleitet das Produkt von der Planung über Entwicklung, Herstellung und Lieferung bis zur Wartung. Sie geht von Zweckbestimmung, vorhersehbarer Verwendung, Einsatzumgebung und Nutzungsdauer aus, legt fest, welche Anforderungen aus Anhang I Teil I Nr. 2 gelten und wie sie umgesetzt werden, und wird während des Unterstützungszeitraums fortgeschrieben, sobald neue Schwachstellen oder Informationen Dritter bekannt werden. Nachweis: freigegebene, versionierte Risikobewertung in der technischen Dokumentation mit Begründung für jede nicht anwendbare Anforderung und Änderungsprotokoll.		
24	Gebotene Sorgfalt bei Komponenten Dritter, auch bei Open Source Art. 13 Abs. 5	Bevor eine zugekaufte oder frei verfügbare Komponente in das Produkt kommt, wird geprüft, ob sie dessen Cybersicherheit gefährden kann: Herkunft, Pflegezustand, bekannte Schwachstellen, Supportzusagen und Lizenz. Das gilt ausdrücklich auch für Open-Source-Software, die nicht im Rahmen einer Geschäftstätigkeit bereitgestellt wurde. Nachweis: Auswahlkriterien für Komponenten, Prüfprotokolle je Komponente, Lieferantenbewertung und kontrollierte Aufnahme in den Build.		

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
25	Schwachstellen in Komponenten an deren Hersteller oder Betreuer melden und Korrekturen teilen Art. 13 Abs. 6	Findet das eigene Team eine Schwachstelle in einer eingebauten Komponente, auch in einer Open-Source-Komponente, wird sie an die Stelle gemeldet, die die Komponente herstellt oder pflegt, und im eigenen Produkt wie jede andere Schwachstelle nach Anhang I Teil II behandelt. Wurde selbst ein Fix entwickelt, geht der Code oder die Beschreibung an diese Stelle zurück, wo sinnvoll maschinenlesbar. Nachweis: Meldeweg je Komponente, Protokoll der Meldungen an Upstream-Projekte und Lieferanten, Verweis auf den internen Schwachstellenfall.		
26	Unterstützungszeitraum festlegen, angeben und Schwachstellen darin wirksam behandeln Art. 13 Abs. 8 und 19	Der Unterstützungszeitraum richtet sich nach der erwarteten Nutzungsdauer und den berechtigten Erwartungen der Nutzer und beträgt grundsätzlich mindestens fünf Jahre, bei kürzerer Nutzungsdauer entsprechend weniger. Die Gründe für die Festlegung stehen in der technischen Dokumentation. Beim Kauf ist das Enddatum mindestens mit Monat und Jahr klar erkennbar, und wo technisch möglich erhalten Nutzer eine Mitteilung, wenn der Zeitraum endet. Während des Zeitraums werden Schwachstellen nach Anhang I Teil II behandelt, gestützt auf eine Strategie zur koordinierten Offenlegung. Nachweis: dokumentierte Festlegung mit Begründung, Angabe auf Produkt, Verpackung oder Website, Schwachstellenprozess mit CVD-Richtlinie.		
27	Bereitgestellte Sicherheitsaktualisierungen mindestens zehn Jahre verfügbar halten Art. 13 Abs. 9	Jede Sicherheitsaktualisierung, die Nutzern im Unterstützungszeitraum bereitgestellt wurde, bleibt ab ihrer Bereitstellung mindestens zehn Jahre abrufbar, oder länger, wenn der Unterstützungszeitraum noch länger läuft. Dazu gehören ein dauerhaftes Update-Archiv, gesicherte Signaturschlüssel und Prüfsummen sowie eine Planung für den Wechsel von Download-Plattformen. Nachweis: Archivkonzept mit Aufbewahrungsfrist, Liste der bereitgestellten Updates mit Datum, Stichprobe zur Abrufbarkeit.		
28	Technische Dokumentation und EU-Konformitätserklärung aufbewahren Art. 13 Abs. 13	Technische Dokumentation und EU-Konformitätserklärung werden nach dem Inverkehrbringen mindestens zehn Jahre aufbewahrt, oder für die Dauer des Unterstützungszeitraums, wenn dieser länger ist, und der Marktüberwachungsbehörde auf Verlangen vorgelegt. Die Aufbewahrung umfasst alle Fassungen je Produktversion, bleibt bei Systemwechseln lesbar und ist gegen Veränderung geschützt. Nachweis: Ablageort und Aufbewahrungsregel, Versionsliste der Dokumentation je Produkt, Zugriffskonzept.		
29	Informationen und Anleitungen für Nutzer beifügen und verfügbar halten Art. 13 Abs. 18	Dem Produkt liegen die Angaben nach Anhang II bei, auf Papier oder elektronisch, in einer für Nutzer und Behörden leicht verständlichen Sprache, klar und lesbar, sodass Installation, Betrieb und Nutzung sicher gelingen. Die Informationen bleiben mindestens zehn Jahre nach dem Inverkehrbringen oder für den längeren Unterstützungszeitraum verfügbar; online bereitgestellte Fassungen sind zugänglich und benutzerfreundlich. Nachweis: Nutzerinformation je Produktversion mit Abgleich gegen Anhang II, Sprachfassungen, Veröffentlichungsort und Aufbewahrungsregel.		

Meldepflichten der Hersteller (Art. 14)

Nr.	Anforderung	Was eine Prüfung sehen will	Status	Nachweis / Notiz
30	Aktiv ausgenutzte Schwachstellen fristgerecht melden (24 Stunden, 72 Stunden, 14 Tage) Art. 14 Abs. 1, 2 und 7	Erfährt der Hersteller von einer aktiv ausgenutzten Schwachstelle im Produkt, meldet er sie über die einheitliche Meldeplattform der ENISA gleichzeitig an das zuständige koordinierende CSIRT und die ENISA: eine Frühwarnung innerhalb von 24 Stunden mit den betroffenen Mitgliedstaaten, eine Schwachstellenmeldung innerhalb von 72 Stunden mit Angaben zu Produkt, Art der Ausnutzung und Gegenmaßnahmen sowie einen Abschlussbericht spätestens 14 Tage, nachdem eine Korrektur oder Risikominderung verfügbar ist. Zuständig ist das CSIRT des Mitgliedstaats der Hauptniederlassung. Nachweis: Meldeprozess mit Rollen und Vertretung, Zugang zur Meldeplattform, Vorlagen für die drei Stufen, Protokoll von Übungen oder echten Meldungen.		
31	Schwerwiegende Sicherheitsvorfälle mit Auswirkung auf die Produktsicherheit melden (24 Stunden, 72 Stunden, ein Monat) Art. 14 Abs. 3, 4 und 5	Schwerwiegend ist ein Vorfall, wenn er die Fähigkeit des Produkts beeinträchtigt oder beeinträchtigen kann, Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit sensibler oder wichtiger Daten oder Funktionen zu schützen, oder wenn er zum Einschleusen oder Ausführen von Schadcode im Produkt oder beim Nutzer geführt hat oder führen kann. Dann gehen über die einheitliche Meldeplattform gleichzeitig an CSIRT und ENISA: eine Frühwarnung binnen 24 Stunden mit der Angabe, ob ein rechtswidriges oder böswilliges Handeln vermutet wird, eine Vorfallsmeldung binnen 72 Stunden mit erster Bewertung und Gegenmaßnahmen und ein Abschlussbericht innerhalb eines Monats nach dieser Meldung. Nachweis: Bewertungskriterien für die Einstufung, Ablauf vom Erkennen bis zur Meldung, Vorlagen, Übungsprotokoll.		
32	Betroffene Nutzer über Schwachstelle oder Vorfall und mögliche Gegenmaßnahmen informieren Art. 14 Abs. 8	Nach Kenntnis einer aktiv ausgenutzten Schwachstelle oder eines schwerwiegenden Vorfalls werden die betroffenen Nutzer, falls angebracht alle Nutzer, informiert, und zwar auch darüber, was sie selbst zur Risikominderung oder Behebung tun können, wo sinnvoll in einem strukturierten, maschinenlesbaren Format wie CSAF. Unterbleibt die Information, kann das koordinierende CSIRT die Nutzer selbst unterrichten. Nachweis: Kommunikationsplan mit Kanälen und Zielgruppen, Vorlage für Sicherheitshinweise, veröffentlichte Advisories mit Datum.		

Über diese Vorlage

Vorlagenversion 1.0-eb06febc
Stand der Inhalte 12.11.2026
Herausgeber Erstellt mit Complass, https://complass.eu

Rechtsgrundlage (Stand): Verordnung (EU) 2024/2847, amtliche deutsche Fassung auf EUR-Lex mit den Berichtigungen ABl. L 2025/90555, ABl. L 2025/90828 und ABl. L 2026/90667 (modules/lawtexts, abgerufen am 06.10.2026), Durchführungsverordnung (EU) 2025/2392, Delegierte Verordnungen (EU) 2025/1535 und 2026/881, Art. 104 der Verordnung (EU) 2025/327 (EHDS), Richtlinie (EU) 2024/2853, BSI TR-03183-2 Version 2.1.0. Leitlinien der Kommission C(2026) 5252 vom 27.07.2026 (Abschnitte 3.2, 4, 5, 8.1, 9.1 und 9.3.1 am 12.11.2026 im Volltext abgeglichen).

Diese Vorlage ist keine Rechtsberatung. Sie ersetzt nicht die Prüfung, welche Anforderungen für Ihr Unternehmen gelten, und garantiert kein Prüfungs- oder Zertifizierungsergebnis.

Lizenz: Creative Commons Namensnennung 4.0 International (CC BY 4.0). Sie dürfen die Vorlage verwenden, ändern und weitergeben, auch kommerziell, wenn Sie die Quelle nennen. Namensnennung: „Vorlage: Complass (complass.eu), CC BY 4.0“. https://creativecommons.org/licenses/by/4.0/deed.de