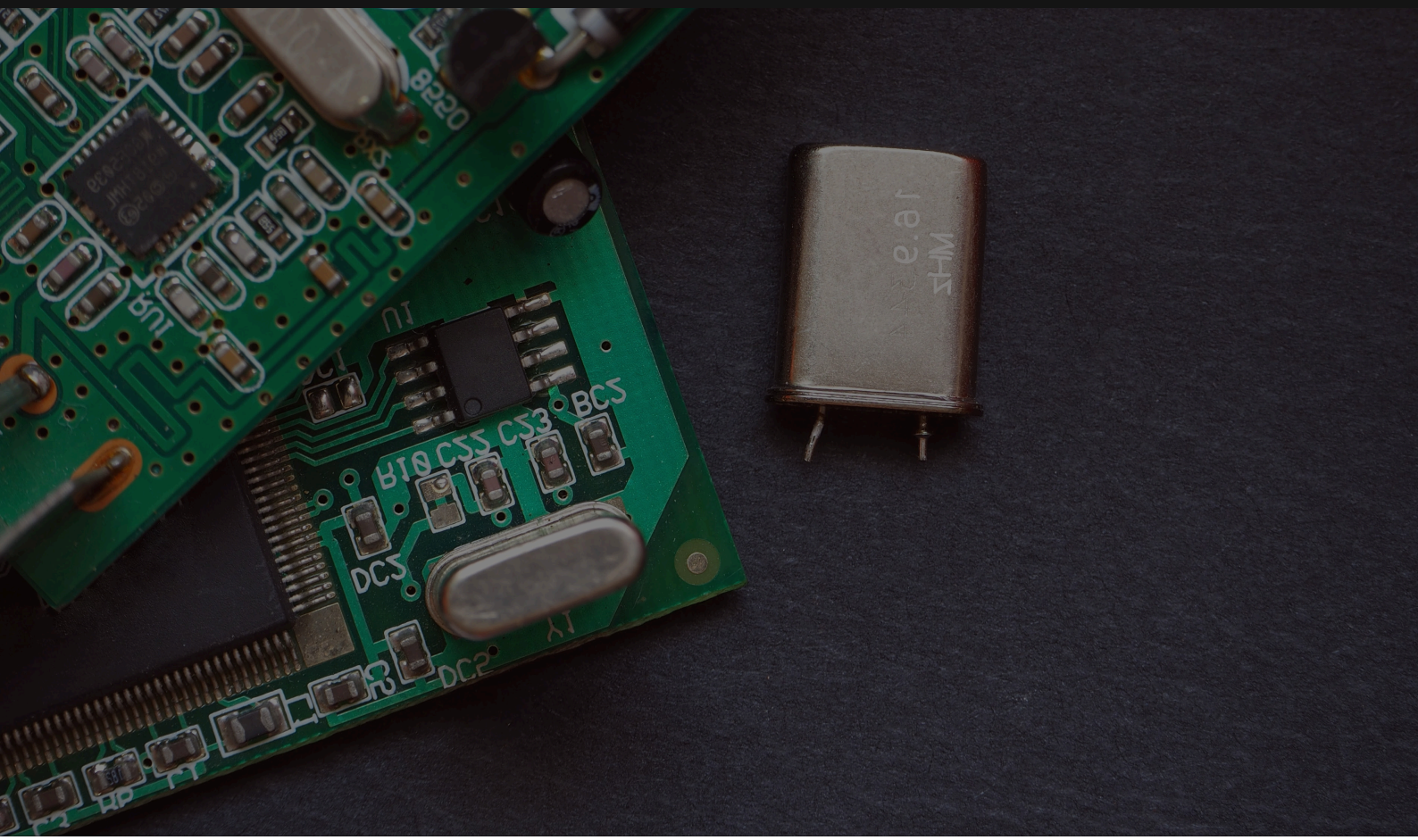
KiviCore

We secure embedded systems



Cyber Resilience Act (CRA) Checkliste für embedded Systeme

Acht wichtige Schritte zur CRA Konformität

Der Cyber Resilience Act (CRA) ist eine EU-Verordnung zur Verbesserung der Cybersicherheit digitaler Produkte und Dienstleistungen. Für Unternehmen ist es entscheidend, die Anforderungen zu verstehen, um embedded Systeme effektiv zu schützen. Hier sind acht wichtige Schritte, auf die sich Hersteller eingebetteter Produktsysteme konzentrieren sollten.

Produktklassifizierung

Hersteller sollten zunächst prüfen, ob Ihre Produkte von der CRA betroffen sind und welcher Kategorie sie zuzuordnen sind. Die Verordnung unterscheidet zwischen Standardprodukten und wichtigen und kritischen Produkten mit digitalen Elementen. Dadurch wird der Anspruch an die Cybersicherheits-Anforderungen und das erforderlichen Konformitätsbewertungsverfahren bestimmt. Die Standardkategorie umfasst alle Produkte mit digitalen Elementen. Andere Produkte werden in den Anhängen III und IV als wichtige und kritische Produkte aufgeführt.

Wichtige Produkte mit digitalen Elementen Klasse I

- Identitätsmanagementsysteme sowie Software und Hardware für die Verwaltung privilegierter Zugriffe, einschließlich Lesegeräte für die Authentifizierung und Zugangskontrolle, auch biometrische Lesegeräte
- eigenständige und eingebettete Browser
- Passwort-Manager
- Software für die Suche, Entfernung und Quarantäne von Schadsoftware
- Produkte mit digitalen Elementen mit der Funktion eines VPNs
- Netzmanagementsysteme
- Systeme für die Verwaltung von Sicherheitsinformationen und -ereignissen
- Bootmanager
- Public-Key-Infrastrukturen und Software für die Ausstellung digitaler Zertifikate
- physische und virtuelle Netzschnittstellen
- Betriebssysteme
- Router, Modems für die Internetanbindung und Switches
- anwendungsspezifische integrierte Schaltungen (ASIC) und FPGA (Field Programmable Gate Array) mit sicherheitsrelevanten Funktionen

- Mikroprozessoren mit sicherheitsrelevanten Funktionen
- Mikrocontroller mit sicherheitsrelevanten Funktionen
- virtuelle Assistenten für die intelligente häusliche Umgebung mit allgemeinem Zweck
- Produkte für die intelligente häusliche Umgebung mit Sicherheitsfunktionen, einschl. intelligenter Türschlösser, Sicherheitskameras, Babyüberwachungssysteme und Alarmanlagen
- mit dem Internet verbundenes Spielzeug, das unter die Richtlinie 2009/48/EG des Europäischen Parlaments und des Rates (1) fällt und über Funktionen zur sozialen Interaktion oder zur Ortung verfügt
- am Körper tragbare Produkte, die zum Zwecke der Gesundheitsüberwachung (z. B. Tracking) bestimmt sind und nicht unter die Verordnungen (EU) 2017/745 oder (EU) 2017/746 fallen, oder am Körper tragbare Produkte, die für die Verwendung durch und für Kinder bestimmt sind

Wichtige Produkte mit digitalen Elementen Klasse II

- Hypervisoren und Container-Runtime-Systeme, die eine virtualisierte Ausführung von Betriebssystemen und ähnlichen Umgebungen unterstützen
- Firewalls, Intrusion-Detection-Systeme und Intrusion-Prevention-Systeme
- manipulationssichere Mikroprozessoren
- manipulationssichere Mikrocontroller

Kritische Produkte mit digitalen Elementen

- Hardwaregeräte mit Sicherheitsboxen
- Smart-Meter-Gateways in intelligenten Messsystemen im Sinne des Artikels 2 Nummer 23 der Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates (1) sowie andere Geräte für fortgeschrittene Sicherheitszwecke, einschließlich der sicheren Kryptoverarbeitung

Grundlegende Anforderungen

Die CRA enthält Anforderungen und Verpflichtungen für alle regulierten Produkte. Die Anforderungen können in zwei Kategorien unterteilt werden: Anforderungen an die Produktsicherheit und an die Behandlung von Schwachstellen. Jede Anforderung kann mehrere Schritte enthalten, und Produkte können spezifische Anforderungen haben. Welche Maßnahmen nötig sind und wie sie umgesetzt werden sollten, wird im Regelfall nach einer vorhergehende Bedrohungsanalyse und Risikobewertung des Produkts bestimmt. Wenn Sie Unterstützung benötigen, kommen Sie auf uns zu.

Teil I Cybersicherheitsanforderungen in Bezug auf Produkteigenschaften

Anforderung	Beschreibung
Schutz vor Sicherheits-lücken	Das Produkt muss vor der Veröffentlichung frei von bekannten Schwachstellen sein. Produkte müssen getestet, Schwachstellen behoben und die Testergebnisse in der Dokumentation bereitgestellt werden.
Sichere Standard-konfiguration	Das Produkt muss mit einer sicheren Standardkonfiguration ausgeliefert werden. Ist das Produkt konfigurierbar, muss es in den Originalzustand zurückgesetzt werden, wobei alle Benutzerdaten gelöscht werden. Sicherheitsrelevante Daten dürfen nicht fest codiert sein.
Sicherheits-updates	Sicherheitsupdates müssen bereitgestellt werden, um Sicherheitslücken zu beheben. Hersteller müssen sicherstellen, dass (fast) alle Komponenten updatefähig sind. Update-Funktionen müssen eine sichere Installation, automatische Update-Mechanismen mit Opt-out- und Verzögerungsfunktion gewährleisten.
Zugangs-kontrolle	Authentifizierung und Identitätsmanagement müssen eingesetzt werden, um unbefugten Zugriff zu verhindern. Maßnahmen wie sichere Passwortgenerierung, bewährte Kryptografie und die Verhinderung von Brute-Force-Angriffen müssen angewendet werden. Fehlgeschlagene Authentifizierungsversuche müssen gemeldet und für Benutzer sichtbar sein.

Anforderung	Beschreibung
Vertraulichkeit von Daten	Für sichere Kommunikation personenbezogener oder kritischer Daten müssen kryptografische Verfahren eingesetzt, gespeicherte Daten durch Verschlüsselung geschützt und sichere Verwaltungsprozesse für die vom Hersteller generierten Daten eingehalten werden.
Integrität von Daten	Daten müssen vor Manipulation geschützt werden. Das Produkt muss seine Integrität selbst überprüfen und bei Kompromittierung eine Wiederherstellung ermöglichen, die atomare Installation von Plug-ins ermöglichen, die Deinstallation zulassen und die Integrität durch sichere Verwaltung der Systemressourcen wahren.
Daten-minimierung	Nur unbedingt notwendigen Daten sollen erhoben und verarbeitet werden.
Verfügbarkeit von Funktionen	Wesentliche und grundlegende Funktionen müssen jederzeit geschützt sein. Das Produkt muss in der Standardkonfiguration funktionieren, den sicheren Betrieb nach Unterbrechungen wieder aufnehmen und die Kernfunktionen auch ohne Netzwerk aufrechterhalten.
Minimierung von negativen Effekten	Andere Systeme sollen geschützt werden, indem die Auswirkungen auf sie minimiert werden. Das Produkt muss die Netzwerkressourcen ordnungsgemäß verwalten und Fehlerreaktionen ermöglichen.
Möglichst geringe Angriffsfläche	Geräte müssen minimale Angriffsflächen inkl. externer Schnittstellen bieten. Unnötige Schnittstellen, Dienste und Debug-Funktionen sollen deaktiviert und durch autorisierte Benutzer reaktiviert werden können.
Möglichst geringe Auswirkungen im Ernstfall	Das Produkt muss mit den geringsten Berechtigungen betrieben werden und detaillierte Schnittstellenberechtigungen erzwingen.
Aufzeichnung und Überwachung	Das Produkt muss Änderungen an Sicherheits-einstellungen, Benutzerauthentifizierungen, Dienststatus und Netzwerkdaten überwachen und protokollieren. Autorisierte Nutzer können die Überwachung deaktivieren.

Teil II Anforderungen an die Behandlung von Schwachstellen

Anforderung	Beschreibung
Schwachstellen identifizieren und dokumentieren	Schwachstellen und Komponenten, einschließlich einer Software-Stückliste, müssen dokumentiert werden.
Sicherheitslücken beheben	Hersteller müssen Schwachstellen umgehend durch Updates oder Abhilfemaßnahmen beheben.
Regelmäßige Tests und Überprüfungen	Hersteller müssen die Produktsicherheitsmechanismen und -komponenten auf korrekte Funktion regelmäßig prüfen, testen und dokumentieren.
Behobene Sicherheitslücken veröffentlichen	Der Hersteller muss die Nutzer über Schwachstellen und deren Auswirkungen informieren und Abhilfe schaffen, indem er Sicherheitshinweise in maschinenlesbarer Form bereitstellt.
Offenlegung von Sicherheitslücken	Der Hersteller muss einen Prozess zur Offenlegung von Sicherheitslücken gemäß den Vorgaben veröffentlichen und implementieren.
Informationen über Schwachstellen weitergeben	Der Hersteller muss einen Prozess zur Offenlegung von Sicherheitslücken gemäß den Vorgaben veröffentlichen und implementieren.
Sichere Verteilung von Updates	Der Hersteller stellt einen Mechanismus für die sichere Verteilung von Updates gemäß den Vorgaben bereit.
Bereitstellung von Updates	Der Hersteller muss Aktualisierungsmechanismen und Benutzerdokumentationen für die Anwendung von Aktualisierungen gemäß den Vorgaben bereitstellen.

Dokumentation

Die CRA gibt an, welche Dokumente für Produkte erforderlich sind, um die Anforderungen zu erfüllen. Dazu gehört die technische Dokumentation, eine Software-Stückliste, klare Benutzerinformationen und -anweisungen. Die Dokumentation muss mindestens 10 Jahre lang von den Marktüberwachungsbehörden oder für den Rest der Unterstützungszeit, je nachdem, welcher Zeitraum länger ist, beibehalten werden.

Technische Dokumentation

- Allgemeine Produktbeschreibung
  - Beabsichtigter Anwendungszweck des Produkts
  - Cybersicherheitsrelevante Softwareversionen
  - Bilder und Abbildungen für Hardware (extern/intern)
  - Benutzerinformationen und -anweisungen

- Information über Entwurfs-, Entwicklung, Produktions- und Schwachstellenbehandlungsprozess
  - Entwurfsdaten, Systemarchitektur, Zeichnungen/Schemata
  - Umgang mit Anfälligkeit, Offenlegungsrichtlinien für Verwundbarkeit, Aktualisierungsmechanismen, Kontaktadressen

- Produktions-, Überwachungs- und Validierungsprozessinformationen

- Bewertung von Cybersicherheitsrisiken und Anwendung der grundlegenden Anforderungen während des gesamten Lebenszyklus

- Grundlage für die Bestimmung der Unterstützungszeit

- Verwendete angewendete harmonisierte Standards, Spezifikationen oder EU -Cybersicherheitszertifizierungen oder wenn nur teilweise angewandt Erklärung zu alternative Lösungen und anderen technische Spezifikationen

- Testberichte, die die Einhaltung der Cybersicherheitsanforderungen und das Verwundbarkeitsmanagement bestätigen

Informationen und Anleitungen für den Nutzer

- Name des Herstellers, eingetragener Handelsname/Marke, postalische und digitale Kontaktadresse (E-Mail/Website, falls verfügbar)
- Zentrale Anlaufstelle für die Meldung von Schwachstellen und den Zugriff auf die Richtlinie zur koordinierten Offenlegung von Schwachstellen
- Produktname, -typ und -identifizierende Angaben
- Verwendungszweck, Hauptfunktionen, Sicherheitseigenschaften und bereitgestellte Sicherheitsumgebung
- Bekannte oder vorhersehbare Risiken bei beabsichtigtem oder vernünftigerweise vorhersehbarem Missbrauch
- (Falls zutreffend) URL zur EU-Konformitätserklärung
- Art und Dauer des technischen Sicherheitssupports, einschließlich Updates und Schwachstellenbehandlung.
- Anleitung oder URL zu
  - Sicherheitsmaßnahmen während der Einrichtung und Nutzung
  - Auswirkungen von Änderungen auf die Datensicherheit
  - Installation von Sicherheitsupdates
  - Sichere Außerbetriebnahme des Produkts und Datenlöschung
  - Deaktivierung der automatischen Installation von Sicherheitsupdates
  - Informationen, die für die Integration in andere digitale Produkte zur Erfüllung der Cybersicherheits-/Dokumentationsanforderungen erforderlich sind
- Zugriff auf die Software-Stückliste (falls vorhanden).

Fazit

Die CRA setzt neue Standards für die Cybersicherheit eingebetteter Systeme und verpflichtet Hersteller zu strengeren Sicherheitsmaßnahmen sowie zur Einhaltung von Risikobewertungen, sicheren Designpraktiken und kontinuierlichem Schwachstellenmanagement. Sobald die Verordnung in Kraft tritt, müssen Unternehmen diese Anforderungen umsetzen, um ihre Produkte zu schützen und die EU-Marktstandards zu erfüllen. Die CRA stellt zwar Herausforderungen dar, bietet Herstellern aber auch die Möglichkeit, die Sicherheit ihrer embedded Systeme und Produkte zu verbessern.

> Wie wir helfen können

- Bedrohungs- und Risikobewertungen
- Architektur- und Gap-Analysen
- Implementierung von für Sicherheitsfunktionen
- Unterstützung bei Dokumentation und Tests

Brauchen Sie Hilfe? Werfen Sie einen Blick auf unsere CRA-Services.

Services