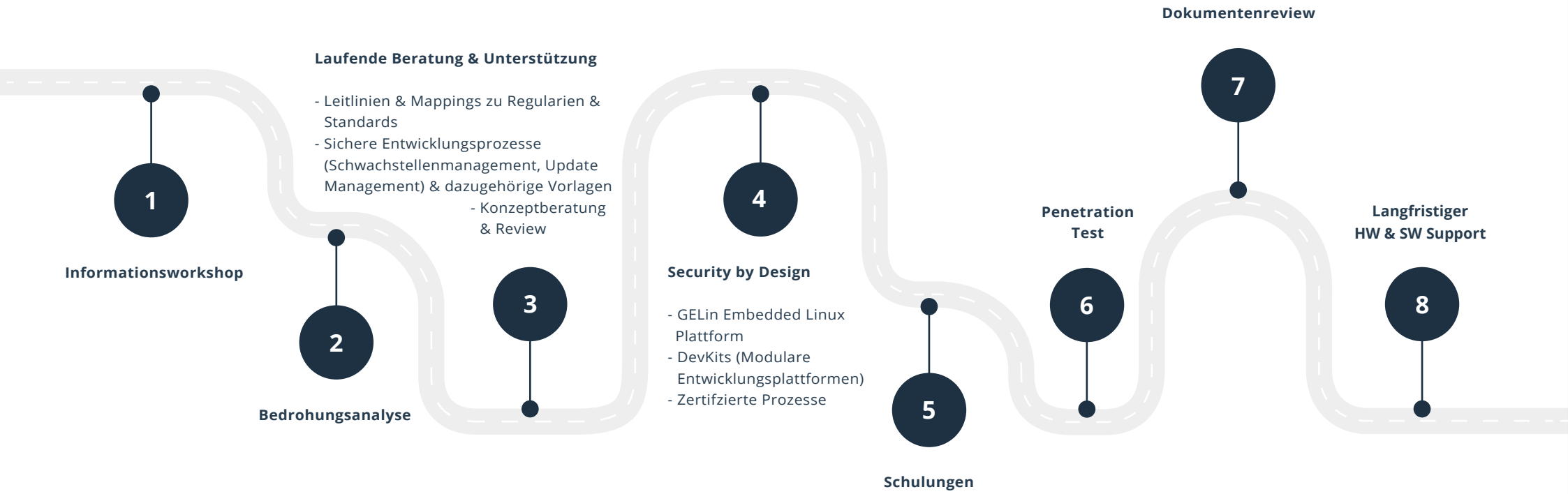
LIMES SECURITY

GINZINGER electronic systems

BEREIT FÜR DEN CYBER RESILIENCE ACT?

WHITEPAPER - TEIL 1 GRUNDLAGEN

CUSTOMER JOURNEY



LEISTUNGSBESCHREIBUNG

LIMES SECURITY

Als führender OT-Security-Experte im deutschsprachigen Raum unterstützt Limes Security Unternehmen bei der sicheren Entwicklung industrieller Produkte und Lösungen.

Zur strukturierten und praxisnahen Umsetzung des Cyber Resilience Acts bietet Limes Security ein breites Spektrum an unterstützenden Leistungen – von der ersten Orientierung bis hin zur technischen Umsetzung und Schulung:

- Informationsworkshops
- Leitlinien & Mappings
- Bedrohungsanalysen
- Konzepterstellung & Review
- Templates für Prozesse, Analysen & Best Practices
- Einführung von sicheren Produktentwicklungsprozessen
- Workshops & Trainings
- Security Tests
- Laufende Beratung & Unterstützung

Die angebotenen Leistungen greifen ineinander und ermöglichen eine strukturierte, nachvollziehbare und praxisgerechte Umsetzung der CRA-Anforderungen – abgestimmt auf individuelle Produkt- und Unternehmensbedürfnisse.

Ziel ist es, als Partner bestmöglich bei der effizienten Entwicklung eines sicheren, CRA-konformen Produkts zu unterstützen.

Im Rahmen der Limes Academy werden darüber hinaus praxisnahe OT-Security Ausbildungen und Zertifizierungen angeboten – für Fachkräfte, die Security nicht nur verstehen, sondern aktiv gestalten wollen. Zwei besonders relevante Trainings im Kontext des Cyber Resilience Acts sind:

- SEC.311 Sichere Entwicklungsprozesse für OT und (I)IoT
- SEC.331 Sichere Embedded & (I)IoT-Produkte

GINZINGER electronic systems

Ginzinger electronic systems unterstützt Hersteller bei der CRA-konformen Entwicklung sicherer Embedded-Systeme mit einer praxisbewährten, integrierten Lösungslandschaft.

– GELin (Ginzinger Embedded Linux) - Plattform

Robuste Embedded-Linux als Basis maßgeschneiderter Produkte mit Secure Boot, Partitionierung, Sicherheitsfunktionen, Software-Stücklisten und Update-Funktionen.

– Security-by-Design

Sicherheitsmechanismen wie Verschlüsselung, Zugriffskontrolle und Integritätsprüfung werden von Beginn an in Hard- und Software integriert, für eine konforme Umsetzung des Cyber Resilience Act.

– Hardware & Plattformdesign

Entwicklung und Produktion sicherer, industrietauglicher Hardware mit Fokus auf Langzeitverfügbarkeit, Manipulationsschutz und geprüften Komponenten.

– Langfristige Wartung & Pflege

Langfristig gewartete Soft- und Hardware Plattform, Sicherheits-Updates (lokal/OTA) für den gesamten Produktlebenszyklus, zuverlässig, reproduzierbar und auditierbar.

– Protokollierung & Compliance

Robustes Logging, ISO-konforme Prozesse und Unterstützung bei Audits, Risikoanalysen und Incident Response.

INHALT TEIL 1

1. WAS HERSTELLER JETZT WISSEN MÜSSEN

1.1 Was sind Produkte mit digitalen Elementen?

2. WOZU DIENT DER CRA? WAS IST SEIN ZIEL?

2.1 Hintergrund: Warum der CRA notwendig wurde
2.2 CRA sorgt für Sicherheit über den gesamten Lebenszyklus
2.3 CRA sorgt für einheitliche Vorgaben für einen fairen Wettbewerb
2.4 CRA sorgt für transparente Informationen für Nutzer:innen
2.5 Unterstützung für kleine Unternehmen

3. FAKTEN: WER IST VOM CRA BETROFFEN?

3.1 Ausnahmen vom CRA
3.2 Hohe Relevanz für Unternehmen

4. WAS SIND DIE ANFORDERUNGEN DES CRA?

4.1 Risikobasiertes Sicherheitskonzept
4.2 SBOM & Schwachstellenmanagement
4.3 Anforderungen an die Hardware (nach CRA)
4.4 Anforderungen des CRA an Embedded Software
4.5 So können wir Sie bei der Umsetzung unterstützen

CYBER RESILIENCE ACT
WAS HERSTELLER JETZT WISSEN MÜSSEN

Der Cyber Resilience Act (CRA) wurde seitens des Europäischen Rates im Oktober 2024 verabschiedet. Damit definieren sich zwei Stichtage, welche für Hersteller, Importeure und Händler von Produkten mit digitalen Elementen von Relevanz sind:

Ab 11. September 2026

gilt eine Meldepflicht. Unternehmen müssen schwerwiegende Sicherheitsvorfälle, sowie aktiv ausgenutzte Schwachstellen, die die Cybersicherheit eines Produkts betreffen, an nationale oder europäische Behörden melden.

Ab 11. Dezember 2027

müssen alle technischen und organisatorischen Anforderungen des CRA erfüllt sein. Dazu zählen u. a. risikobasierte Sicherheitsmaßnahmen und die Bereitstellung von Sicherheitsupdates über den gesamten, zu definierenden Unterstützungszeitraum hinweg.

CE

Damit gilt: Ein Produkt mit digitalen Elementen darf ab 11.12.2027 nur dann mit dem CE-Kennzeichen versehen und im EU-Binnenmarkt vertrieben werden, wenn es den Anforderungen des CRA entspricht.

Bei Verstößen drohen empfindliche Bußgelder: Bis zu 15 Millionen Euro oder 2,5 % des weltweiten Jahresumsatzes des Unternehmens – je nachdem, welcher Betrag höher ist. Weiters kann die Marktaufsichtsbehörde auch Produkte vom Markt nehmen oder Nachbesserungen fordern.

Bei Verstößen drohen Bußgelder:

15 Mio € oder 2,5%	Artikel 13 & 14
10 Mio € oder 2%	andere Artikel
15 Mio € oder 1%	Falschaussagen

1.1 Was sind Produkte mit digitalen Elementen?

Als Produkt mit „digitalen Elementen" gelten alle Hardware-, sowie Softwareprodukte und deren Datenfernverarbeitungslösungen, welche einen physischen oder logischen Datenaustausch mit anderen Produkten oder Netzwerken temporär oder auch permanent ermöglichen.

Vereinfacht gesagt: Es kann angenommen werden, der CRA gilt für reine Softwareprodukte sowie für Hardwareprodukte, wenn diese über eine Kommunikationsschnittstelle (bei Hardware z.B.: Ethernet, USB, SD-Card, PCIe, ...) verfügen. Und das sowohl für Produkte für Endkunden, als auch für Produkte, die in andere integriert werden. Nur wenige Ausnahmen sind vorgesehen.

In den folgenden Abschnitten wird detaillierter auf zentrale Elemente des CRAs eingegangen, was man als Hersteller von betroffenen Produkten nun tun muss und wie man diese Herausforderungen am Besten angeht.

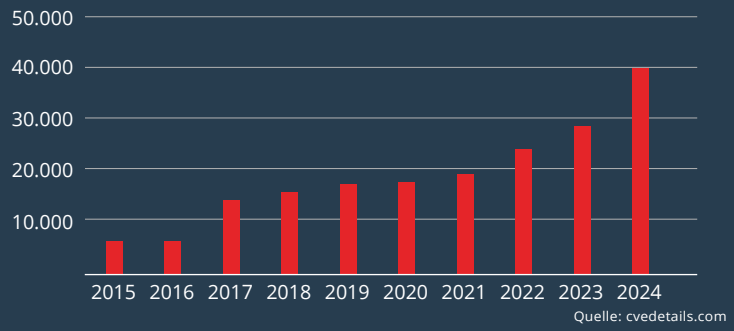
WOZU DIENT DER CRA? WAS IST SEIN ZIEL?

Mit dem Cyber Resilience Act (CRA) verfolgt die EU das Ziel, die Cybersicherheit vernetzter Produkte im Binnenmarkt deutlich zu verbessern. Hersteller, Importeure und Händler werden verpflichtet, Sicherheitsaspekte von Beginn an systematisch zu berücksichtigen. Sowohl bei der Entwicklung, als auch über den gesamten Lebenszyklus eines Produkts hinweg.

2.1 Hintergrund: Warum der CRA notwendig wurde

Die zunehmende Komplexität von Software und die stärkere Vernetzung von Produkten führen dazu, dass Sicherheitslücken immer häufiger auftreten.

Anzahl der gemeldeten Schwachstellen und Risiken (CVE):



Quelle: cvedetails.com

Diese entstehen nicht per se durch schlechtere Entwicklung, sondern durch:

– wachsende technische Komplexität,
– intensivere Tests und Analysen,
– sowie die steigende Anzahl und Professionalität von Angriffen.

Solche Schwachstellen können gravierende Folgen haben: Von Daten- und Know-how-Diebstahl, über Manipulationen, bis hin zu Beeinträchtigungen von Systemen, Infrastrukturen oder gar der physischen Sicherheit von Menschen. Produkte sind besonders gefährdet, wenn Cybersicherheit nicht frühzeitig berücksichtigt wird. Der CRA soll daher sicherstellen, dass Sicherheitslücken bereits vor dem Inverkehrbringen erkannt und beseitigt werden, damit sollen unsichere Produkte so gar nicht erst auf den Markt gelangen.

2.2 CRA sorgt für Sicherheit über den ganzen Lebenszyklus

Cybersicherheit endet nicht mit der Auslieferung eines Produkts. Da sich Bedrohungslagen laufend verändern, verpflichtet der CRA Hersteller dazu,

– Produkte dauerhaft auf neue Schwachstellen zu prüfen und
– über den gesamten Lebenszyklus hinweg Sicherheitsupdates bereitzustellen.

So wird gewährleistet, dass Produkte auch Jahre nach dem Verkauf noch einem aktuellen Sicherheitsstandard entsprechen.

2.3 CRA sorgt für einheitliche Vorgaben für einen fairen Wettbewerb

Regulatorische Anforderungen an die Cybersicherheit sind nicht neu, es gibt solche Regelungen bereits unter anderem für:

– Medizinprodukte (MDR)
– Funkanlagen (RED)
– Maschinen (Maschinenverordnung)

Der CRA setzt somit erstmals eine übergreifende, produktgruppenunabhängige Basis und ermöglicht

– gleiche Wettbewerbsbedingungen für alle Marktteilnehmer und
– ein einheitliches Schutzniveau im EU-Binnenmarkt.

Die Vorgaben gelten sowohl für europäische Anbieter, als auch für internationale Hersteller, die in den EU-Binnenmarkt liefern möchten.

2.4 CRA sorgt für transparente Informationen für Nutzer

Neben der technischen Sicherheit legt der CRA besonderen Wert auf Informationspflichten. Kunden, Betreiber und Integratoren sollen genau wissen,

– wie lange Sicherheitsupdates verfügbar sind,
– wie die sichere Inbetriebnahme und Außerbetriebnahme erfolgen soll,
– wie Sicherheitsfunktionen konfiguriert werden können und
– wo Informationen zu Schwachstellen oder Updates zu finden sind.

Diese Transparenz ermöglicht es, Produkte auch hinsichtlich ihrer Sicherheit zu vergleichen und macht Cybersicherheit zu einem relevanten Kriterium bei der Kaufentscheidung.

2.5 Unterstützung für kleine Unternehmen

Die EU ist sich bewusst, dass vor allem kleine und mittlere Unternehmen (KMU) vor besonderen Herausforderungen stehen. Deshalb sollen nationale Förderprogramme helfen, die Anforderungen des CRA effizient umzusetzen.

FAKTEN:
WER IST VOM CRA BETROFFEN?

Der CRA gilt für alle Produkte mit digitalen Elementen, die erstmals auf dem EU-Binnenmarkt bereitgestellt werden, unabhängig davon, ob sie in Serie oder einzeln gefertigt wurden. Voraussetzung ist, dass der bestimmungsgemäße oder vorhersehbare Gebrauch eine logische oder physische Datenverbindung zu einem Gerät oder Netz einschließt.

„Bereitstellung auf dem Markt“
Als Bereitstellung gilt jede entgeltliche oder unentgeltliche Abgabe eines Produkts im Rahmen einer Geschäftstätigkeit. Dabei ist nicht der Produkttyp, sondern jedes einzelne Produkt entscheidend (Blue Guide CE 2.2).

„Inverkehrbringen“
Das Inverkehrbringen ist die erstmalige Bereitstellung auf dem EU-Markt. Der Zeitpunkt der Inbetriebnahme spielt für den CRA keine Rolle (Blue Guide CE 2.3).

3.1 Ausnahmen vom CRA

Folgende Bereiche sind vom CRA ausgenommen bzw. haben schon eigene, teils wesentlich schärfere Regelungen:

– Produkte, die anderweitig reguliert sind
– Sicherheits- oder Verteidigungsprodukte
– Systeme zur Verarbeitung von Verschlusssachen
– Ersatzteile nach Originalspezifikation
– Prototypen und unfertige Software zu Demonstrations- oder Testzwecken

3.2 Hohe Relevanz für Unternehmen

Es herrscht also für alle Unternehmen, die Produkte mit digitalen Elementen in den EU-Binnenmarkt liefern wollen, Handlungsbedarf.

Wichtig ist:

– Maßgeblich ist der erstmalige Marktzugang in der EU.
– Weiterverkäufe können betroffen sein, wenn sie als Erstbereitstellung gelten.
– Produkte, die nicht für den EU-Markt bestimmt sind, fallen nicht unter den CRA.

Finden Sie heraus, ob Sie oder Ihr Produkt vom CRA betroffen sind:

limessecurity.com/cra-check

WAS SIND DIE ANFORDERUNGEN DES CRA?

Der CRA verpflichtet Hersteller, die Cybersicherheit ihrer Produkte umfassend zu berücksichtigen, sowohl technisch als auch organisatorisch.

Folgende zentrale Anforderungen sind dabei zu erfüllen:

– ein risikobasiertes Sicherheitskonzept
– Software Stückliste (SBoM - Software Bill of Material)
– Schwachstellenmanagement
– Sicherheitsupdates
– die Meldung von Vorfällen
– eine Dokumentation des Produkts

4.1 Risikobasiertes Sicherheitskonzept

Der Cyber Resilience Act (CRA) verlangt, dass Cybersicherheit über den gesamten Produktlebenszyklus hinweg berücksichtigt wird – von der Konzeption über die Entwicklung bis zur Herstellung.

4.1.1 Risikobasierter Ansatz anstatt Detailvorgaben

Der CRA schreibt keine konkreten Maßnahmen vor, sondern überlässt es den Herstellern, geeignete Schutzmaßnahmen auf Basis einer Bedrohungs- und Risikoanalyse selbst zu definieren. Dabei müssen Eintrittswahrscheinlichkeit und potenzielle Auswirkungen von Bedrohungen bewertet werden. Ziel ist es, das verbleibende Restrisiko auf ein vertretbares Maß zu senken – nicht zwingend mit High-End-Maßnahmen, aber angemessen und nachvollziehbar.

4.1.2 Wesentliche Sicherheitsziele gemäß CRA ANHANG I, TEIL 1, ART. 2

Hersteller müssen sicherstellen, dass ihre Produkte unter anderem

– ohne bekannte Schwachstellen und mit sicheren Standardkonfigurationen ausgeliefert werden,
– eine minimale Angriffsfläche bieten und Sicherheitsvorfälle eingrenzen,
– Vertraulichkeit, Integrität und Verfügbarkeit von Daten durch geeignete Schutzmechanismen gewährleisten,
– Sicherheitsupdates ermöglichen, idealerweise automatisch,
– Datensparsamkeit umsetzen – nur notwendige Daten speichern und verarbeiten,
– interne Vorgänge überwachen (z. B. Datenzugriffe, Änderungen) mit Opt-out Möglichkeit für Nutzer:innen
– Nutzern erlauben, eigene Daten sicher und dauerhaft zu löschen.

4.1.3 Umsetzung und Bewertung

Welche Maßnahmen ein Hersteller ergreift, hängt vom individuellen Risikoempfinden ab, sie müssen jedoch dokumentiert und vertretbar sein. Zur Festlegung „Stand der Technik“-gerechter Maßnahmen und zur Durchführung belastbarer Risikoanalysen empfiehlt sich der Miteinbezug externer Expertise.

4.2 SBOM & Schwachstellenmanagement

Der Cyber Resilience Act (CRA) verlangt neben technischen Schutzmaßnahmen auch organisatorische Prozesse zur frühzeitigen Erkennung und Behebung von Sicherheitslücken. Durch eine SBoM gewinnt man einen Einblick darüber, welche Bibliotheken bzw. Softwarebestandteile in welcher Version in einem Produkt vorliegen. Dies ist kein neues Konzept, sondern im Zuge von Lizenzmanagement ein

etablierter Schritt. Besonders im Bereich Embedded Systems bringt dies spezifische Anforderungen mit sich.

4.2.1 Software Bill of Materials (SBoM)

Um Schwachstellen im Produkt schnellstmöglich identifizieren zu können, wird vom CRA die Erstellung einer Software Bill of Materials (kurz SBoM) in standardmäßigen, maschinenlesbaren Formaten vorgeschrieben. Diese kann Kunden zur Verfügung gestellt werden. Sie ist im Falle einer Kontrolle durch die Marktaufsichtsbehörde jedoch bei dieser vorzulegen, wie auch andere, erforderliche Dokumentationen (bspw. die Bedrohungsanalyse).

Die SBoM listet alle Software-Komponenten und Bibliotheken eines Produkts in einem standardisierten, maschinenlesbaren Format auf (z.B. SPDX, CycloneDX). Sie ist ein zentrales Werkzeug zur Identifikation von Schwachstellen. Der CRA fordert, abgesehen von der Existenz einer SBoM, keine direkte weitere Aktion mit dieser. Es hat sich aber bewährt, die SBoM als Basis für die Schwachstellen-Beobachtung zu verwenden.

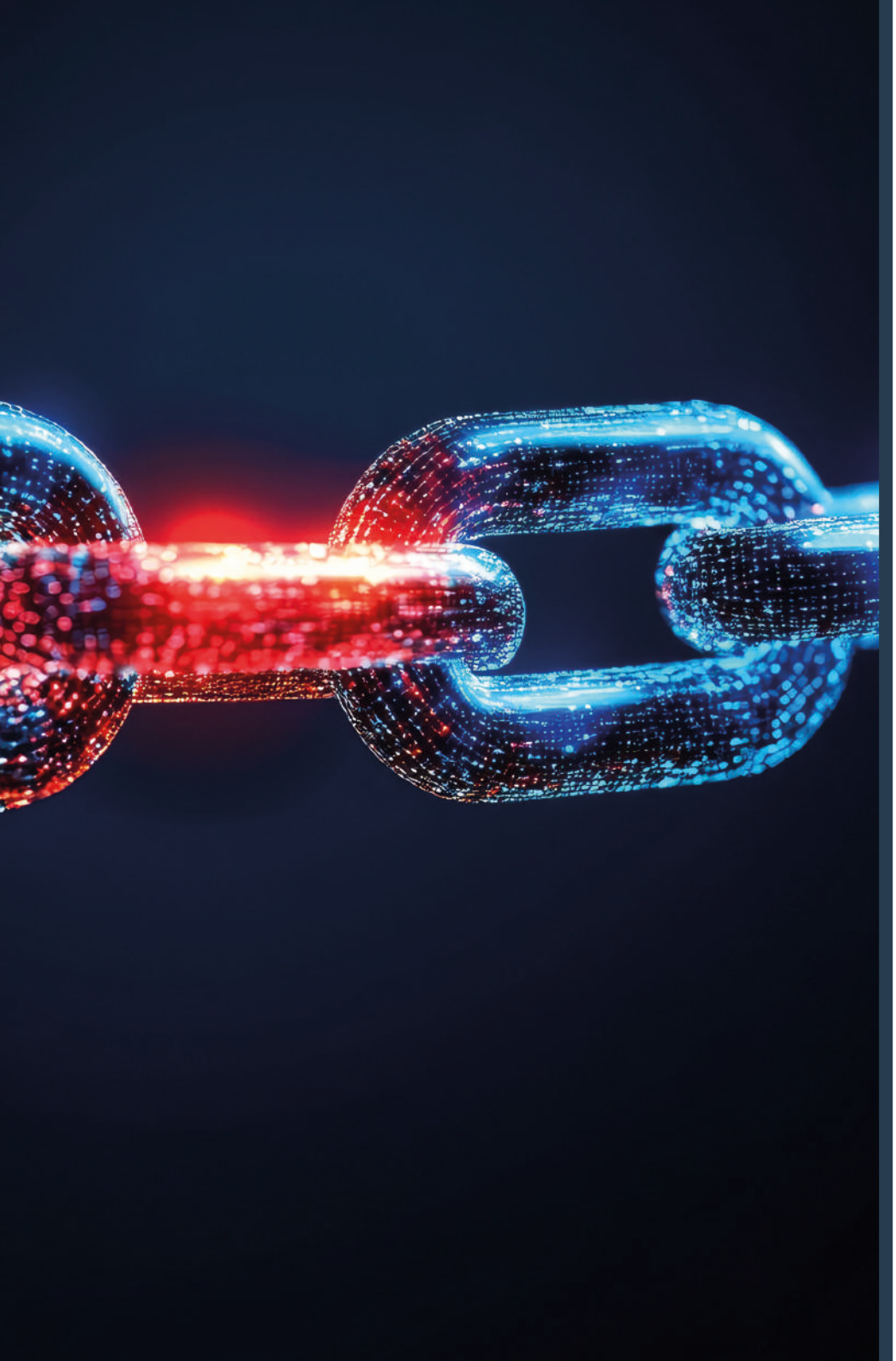
Pflichten und Einsatz:

- Pflicht zur Erstellung und Vorlage gegenüber Behörden
- Freiwillige Weitergabe an Kunden
- Grundlage für automatisiertes Schwachstellenmonitoring

Embedded-relevante Aspekte:

- In Embedded-Systemen häufig durch Buildsysteme oder Embedded Linux Distributionen wie GELin (Ginzinger Embedded Linux) generierbar
- Viele Open-Source-Komponenten sind bereits mit SBoMs verfügbar
- Bei Bare-Metal- oder RTOS-Systemen meist manuell oder mit Spezialtools
- Ressourcenlimits erfordern modulare, effiziente SBoM-Strukturen

Für die Analyse der SBoM hinsichtlich Schwachstellen gibt es ebenso Programme (Open Source wie auch kommerziell), welche Datenbanken nach gemeldeten Schwachstellen durchsuchen und mit einem Dashboard bzw. Bericht die Möglichkeit geben, diese zu analysieren und zu bewerten.
Im Embedded-Bereich bedeutet das oft: lange Produktlebenszyklen und komplexe Lieferketten müssen berücksichtigt werden.



4.2.2 Schwachstellenmanagement

Ein strukturiertes Verfahren zur Bewertung, Bearbeitung und Meldung von Schwachstellen ist Pflicht, denn

– Schwachstellen müssen unverzüglich behoben werden
– Updatefähigkeit (z. B. über OTA oder lokal via USB) ist bei Embedded-Geräten besonders zu planen
– Updates müssen nutzergerecht bereitgestellt werden, auch bei Offline-Systemen

Damit Externe wissen, wo sie Schwachstellen bei Herstellern einmelden können empfiehlt es sich, eine Kontaktstelle auf der eigenen Website einzurichten und dort z.B. über security.txt Angaben zu Kontakt, Reaktionsfristen, Koordination und ggf. Bug-Bounties zu hinterlassen. Falls Schwachstellen gefunden werden, ist auch eine verschlüsselte Kommunikation mit den Entdeckern dringend empfohlen. Andernfalls droht, dass Dritte die Kommunikation abhören und die Schwachstelle umgehend ausnutzen.

Beispiel für Kontaktstelle
(z.B. mittels security.txt auf der Website):

Contact: https://g.co/vulnz

Contact: mailto:security@google.com

Encryption: https://services.google.com/corporate/publickey.txt

Acknowledgments: https://bughunters.google.com/

Policy: https://g.co/vrp

Hiring: https://g.co/SecurityPrivacyEngJobs

Expires: 2030-04-01T00:00:00z

Kurzum: In einer derartigen security.txt ist festgehalten, wann und wie jemand Kontakt aufnehmen kann, sollte eine Schwachstelle gefunden, oder ein Produkt Teil eines Vorfalls geworden sein. Häufig finden sich auch policies, in denen mitunter definiert ist, welche Informationen erfordert werden, unter welchen Fristen eine

koordinierte Schwachstellenveröffentlichung erfolgt, ob Prämien bzw. Bounty's ausgezahlt werden, u.v.m.

Neben der Definition der zentralen Meldestelle (z.B. security@ihrefirma.com) sind auch definierte Abläufe notwendig, um mit einer solchen Meldung umzugehen. Hier müssen die Verantwortlichkeiten und Abläufe geklärt sein.

Folgende Fragen können dabei helfen:

? Wer überprüft die Mail-Adresse, bzw. öffentliche Quellen auf Schwachstellen, die im Produkt enthalten sein könnten?
? Wer führt die Kommunikation bei einer meldepflichtigen Schwachstelle durch?
? Wer entscheidet wie über die Kritikalität und Dringlichkeit?
? Wie etabliere ich ein "lessons learned" aus der Schwachstelle und verbessere langfristig meinen Entwicklungsprozess?
? Wie kommt die Information an die Personen, die Schwachstellen beurteilen, bzw behandeln können?

Die ISO/IEC 30111:2019 definiert hier für einen derartigen Schwachstellenmanagement-Prozess ein Vorgehen, genauso auch wie das Kapitel "Defect-Management" in der IEC 62443-4-1.

4.2.3 Sicherheitsupdates & Meldepflichten (nach CRA)

Hersteller müssen Sicherheitslücken unverzüglich beheben und entsprechende Updates zeitnah bereitstellen. Dies ist Voraussetzung, um regulatorische Meldepflichten zu erfüllen.

Daraus ergeben sich folgende Anforderungen an Sicherheitsupdates:

Verfügbarkeit, Standardverhalten & Informationspflicht

Verfügbarkeit:

– Updates müssen kostenfrei bereitgestellt werden (Ausnahme: maßgeschneiderte Produkte).
– Sie sind über sichere Kommunikationskanäle bereitzustellen (z.B. HTTPS, OTA) bzw. sollten kryptografisch signiert sein, um die Integrität und Authentizät sicherstellen und überprüfen zu können.
– Sie müssen während eines definierten Unterstützungszeitraums zur Verfügung stehen (i. d. R. mindestens 5 Jahre).

Standardverhalten:

– Produkte sollen automatische Sicherheitsupdates in der Standardkonfiguration unterstützen (Opt-out für Nutzer zulässig).
– Wenn möglich: Trennung von Sicherheits- und Funktionsupdates.

Informationspflicht:

– Nutzer müssen – sofern dies die Sicherheit nicht gefährdet – über Art, Auswirkungen und Schwere der Schwachstelle informiert werden.
– Hinweise zu betroffenen Produkten und Handlungsempfehlungen müssen beigefügt werden.

Für Updates und Versionsupdates gilt es folgendes zu beachten:

– Hersteller sind verpflichtet, nur die jeweils aktuellste Version sicher und CRA-konform zu halten.
– Keine Pflicht, ältere Versionen zu patchen – sofern ein kostenfreier Wechsel zur aktuellen Version möglich ist.
– Dies gilt auch für elektronische Produkte wie Embedded-Geräte: Nutzer müssen technisch in der Lage sein, Updates selbst einzuspielen (z.B. via USB, OTA oder Service-Schnittstellen).
– Kostenpflichtige Wartungsverträge oder Update-Services durch Fachpersonal sind weiterhin nützlich, solange das Update auch selbstständig und kostenfrei durchführbar bleibt.

Für maßgeschneiderte Produkte, insbesondere im Embedded Umfeld, sollte von Beginn an eine klare Definition der Produktlebensdauer und des Updatezeitraums durchgeführt werden.

Bei individuell entwickelten Produkten können Hersteller und Kunde abweichende Vereinbarungen zur Updatepolitik treffen, z.B. kürzere Zeiträume, andere Updatewege oder spezifische SLA-Regelungen.

Bei Embedded Devices ist der Updateweg oft technisch eingeschränkt, sichere und verfügbare Updatepfade sind daher frühzeitig zu planen. Auch Geräte ohne permanente Netzwerkverbindung müssen updatefähig bleiben (z.B. durch eine USB Wartungsschnittstelle).

4.2.4 Dokumentationspflichten nach dem CRA

Hersteller müssen für Produkte mit digitalen Elementen eine umfassende, strukturierte Sicherheitsdokumentation erstellen. Sie dient dem Nachweis der Konformität mit Anhang I des Cyber Resilience Act und ist sowohl für Marktaufsichtsbehörden, als auch zur Unterstützung der Nutzer relevant.

Folgende Inhalte sind in der technischen Dokumentation strukturiert und vollständig darzustellen:

– Verwendungszweck des Produkts
– Softwareversionen und eingesetzte Komponenten
– Abbildungen der äußeren und inneren Merkmale bei Hardware
– Systemarchitektur, inkl. Sicherheitsfunktionen
– Beschreibung der Entwicklung, Produktion und Qualitätssicherung

Um die Schwachstellenbehandlung möglichst einfach zu gestalten, muss in der Dokumentation festgehalten sein, wie mit Schwachstellen umzugehen ist. Dazu gehört ein Verfahren zur Behandlung von Schwachstellen. Außerdem ist eine Richtlinie zur koordinierten Offenlegung (Coordinated Vulnerability Disclosure, CVD) notwendig. Es sollte eine technische Lösung für die sichere Verteilung von Updates vorhanden sein. Zusätzlich müssen Kontaktinformationen zur Meldung von Schwachstellen nachgewiesen werden, zum Beispiel über eine *security.txt*.

Weitere Anforderungen an die Dokumentation:

– Eine Software Bill of Materials (SBoM) muss vorliegen und auf Anfrage den Behörden bereitgestellt werden.
– Eine zusammenfassende Bewertung der Cybersicherheitsrisiken für Nutzer ist erforderlich.
– Definition des Unterstützungszeitraums (z.B. für Sicherheitsupdates)
– Eine Liste angewandter und harmonisierter Normen.
– Spezifikationen, Diagramme und Beschreibungen zur Umsetzung der Anforderungen aus Anhang I Teil I & II.

Es gelten folgende Pflichten zur Aufbewahrung & Aktualisierung:

– Die Dokumentation muss mindestens zehn Jahre ab Inverkehrbringen oder während des gesamten Unterstützungszeitraums (je nachdem, welcher Zeitraum länger ist) verfügbar sein.
– Sie ist kontinuierlich zu aktualisieren, z.B. bei neuen Softwareständen, Komponenten oder Sicherheitsmaßnahmen.

4.2.5 Meldepflichten bei Cybersicherheitsvorfällen und Schwachstellen

Hersteller von Produkten mit digitalen Elementen sind verpflichtet, schwerwiegende Cybersicherheitsvorfälle und aktiv ausgenutzte Schwachstellen unverzüglich zu melden.

Die Meldung erfolgt an das jeweils zuständige CSIRT (Computer Security Incident Response Team, von den Mitgliedsstaaten benannt) und an die ENISA (EU-Agentur für Cybersicherheit).

Für Deutschland CERT-Bund (BSI) Link:
https://bsi.bund.de/CERT-Bund

Für Österreich CERT.at Link:
https://www.cert.at

Für Schweiz GovCERT.ch Link:
https://govcert.ch

Zentrale Koordinationsstelle:
ENISA – European Union Agency for Cybersecurity
Website: enisa.europa.eu

Auch betroffene Nutzer oder – je nach Fall – alle Nutzer des Produkts müssen über Vorfälle informiert werden. Dabei gelten unterschiedliche Anforderungen, je nachdem ob es sich um einen Vorfall oder eine Schwachstelle handelt.

Zunächst zu den Meldepflichten bei Cybersicherheitsvorfällen:

- **Innerhalb von 24 Stunden nach Kenntnisnahme:**
  Frühwarnung mit grundlegenden Informationen.

- **Innerhalb von 72 Stunden:**
  Ausführlichere Meldung mit Art des Vorfalls, Risikobewertung und getroffenen Sofortmaßnahmen.

- **Innerhalb von 1 Monat:**
  Abschlussbericht mit vollständiger Analyse, Schweregrad, Auswirkungen und Maßnahmen für Nutzer.

Ein Vorfall gilt als schwerwiegend, wenn er zur Ausführung bösartiger Software führen kann oder die Fähigkeit des Produkts zur Aufrechterhaltung seiner Sicherheitseigenschaften beeinträchtigt ist.

Bei **aktiv ausgenutzten Schwachstellen**, die das Produkt oder darin verwendete Komponenten betreffen, gelten ähnliche Fristen:

- **Innerhalb von 24 Stunden nach Kenntnisnahme:**
  Frühwarnung

- **Innerhalb von 72 Stunden:**
  Meldung mit Informationen zum betroffenen Produkt, Art der Schwachstelle, bisherige Maßnahmen, sowie eine erste Sensibilitätsbewertung.

- **Innerhalb von 14 Tagen nach Verfügbarkeit einer Korrekturmaßnahme:**
  Abschlussbericht mit Beschreibung, Schweregrad, bereitgestellter Lösung (z.B. Sicherheitsupdate) und – wenn möglich – Informationen zu Angreifern oder Angriffsmustern.

Wichtig ist: Eine Schwachstelle gilt nur dann als meldepflichtig, wenn es verlässliche Hinweise auf aktive Ausnutzung durch unbefugte Dritte gibt. Schwachstellen, die z.B.im Rahmen von Penetrationstests gefunden werden, sind davon nicht betroffen.

Klassifizierung, Konformitätsnachweis & Standards

Der CRA stuft Produkte mit digitalen Elementen in unterschiedliche Kategorien ein, die jeweils eigene Anforderungen an den Konformitätsnachweis haben. Ziel ist, das Cybersicherheitsniveau je nach Bedeutung der Kernfunktion risikogerecht abzusichern.

Für nicht klassifizierte Produkte (keine Einstufung als „wichtig“ oder „kritisch“) ist eine **Selbstdeklaration** durch den Hersteller zulässig. Die Anforderungen des CRA müssen eingehalten werden, ein externer Nachweis ist jedoch optional.
Sie können dabei:

– Harmonisierte Normen anwenden,
– Freiwillig eine Cybersicherheitszertifizierung durchführen,
– oder eine Prüfung durch Dritte in Anspruch nehmen.

Wichtige Produkte werden weiter unterteilt:

Klasse I

Selbstdeklaration nur möglich, wenn harmonisierte Normen angewendet werden. Alternativ kann eine Prüfung durch eine benannte Stelle oder eine Cybersicherheitszertifizierung mit Vertrauensstufe „mittel“ erfolgen.

Klasse II

Hier ist zwingend eine Prüfung durch eine externe Konformitätsstelle oder eine gleichwertige Zertifizierung erforderlich.

Kritische Produkte müssen grundsätzlich eine Cybersicherheitszertifizierung durchlaufen, die den Anforderungen des CRA entspricht. Eine Selbstdeklaration ist hier nicht zulässig.

Die Klassifizierung bezieht sich auf die Kernfunktion des Produkts – z.B. ein Passwort-Manager als zentrales Produkt gilt als „wichtig“, wird ein solcher nur als Nebenfunktion verwendet, ist das Produkt selbst nicht zwingend klassifiziert.

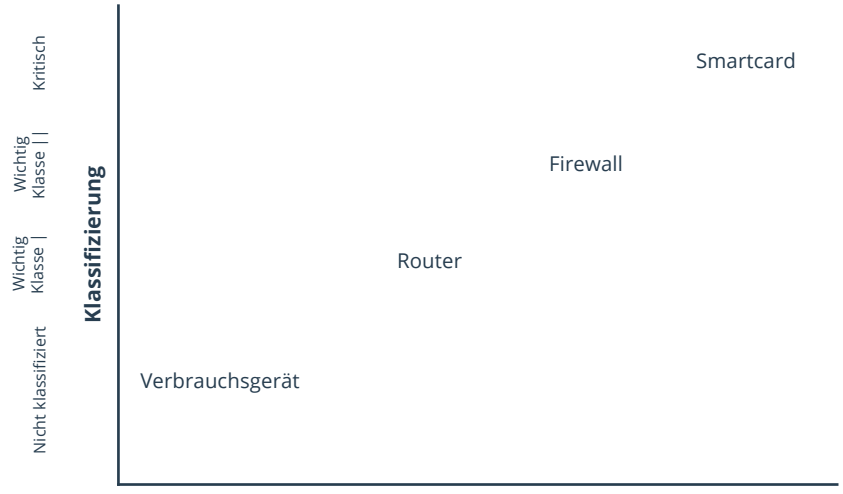
Beispiele für klassifizierte Produkte:

– **Wichtig, Klasse I:**
  VPNs, Betriebssysteme, Router, Passwort-Manager, Smart-Home-Geräte, Internetfähige Spielzeuge, Virenscanner, Mikrocontroller mit Sicherheitsfunktionen
– **Wichtig, Klasse II:**
  Firewalls, Hypervisoren, manipulationssichere Mikrocontroller
– **kritisch:**
  Sicherheitsboxen, Smart-Meter-Gateways, Smartcards oder ähnliche sichere Elemente

Wesentliche Änderungen an Produkten können den Konformitätsstatus beeinflussen. Dazu zählen Änderungen, die

– den bestimmungsgemäßen Zweck verändern
– die Sicherheitsanforderungen aus Anhang I, Teil 1 betreffen
– die Angriffsoberfläche erweitern, etwa durch neue Dienste oder Eingabefelder

Reine visuelle Anpassungen oder reine Bibliotheksupdates ohne Sicherheitswirkung gelten nicht als wesentlich. Die genaue Definition wird durch die EU-Kommission noch spezifiziert.



Risikomatrix: Embedded Systeme vs. CRA-Konformität

Wichtig: Auch Produkte, die vor dem 11. Dezember 2027 in Verkehr gebracht wurden, unterliegen dieser Pflicht, wenn die Änderung danach erfolgt. Hersteller müssen Änderungen daher sorgfältig bewerten und dokumentieren.

4.2.6 Timeline & Sanktionen

Der CRA wird als EU-Verordnung unmittelbar wirksam und bedarf keiner nationalen Umsetzung in den Mitgliedstaaten. Alle Unternehmen, die Produkte mit digitalen Elementen auf dem EU-Binnenmarkt bereitstellen, müssen die Vorgaben einhalten.

Verstöße gegen den CRA haben erhebliche Konsequenzen:

Bei Verstößen gegen Artikel 13 (Herstellerpflichten) oder Artikel 14 (Meldepflichten) drohen:

– Bußgelder bis zu 15 Mio. Euro oder
– 2,5 % des weltweiten Jahresumsatzes – je nachdem, welcher Betrag höher ist.

Zusätzlich können Marktaufsichtsbehörden:

– Produkte vom Markt ausschließen oder zurückrufen
– Die Bereitstellung untersagen
– Nachbesserungen bei bereits ausgelieferten Produkten anordnen

Wichtige Fristen:

Ab 11. September 2026:

Meldepflichten für schwerwiegende Sicherheitsvorfälle und aktiv ausgenutzte Schwachstellen treten in Kraft.

Ab 11. Dezember 2027:

Alle Anforderungen des CRA sind verpflichtend – inklusive Konformitätsbewertung, Dokumentation, Sicherheitsmaßnahmen.

Ab diesem Datum ist eine CE-Kennzeichnung nur noch zulässig, wenn CRA-Konformität nachgewiesen ist!

4.3 Anforderungen an die Hardware (nach CRA)

Der Cyber Resilience Act verpflichtet Hersteller, bereits auf Hardwareebene Cybersicherheit systematisch umzusetzen. Für Embedded-Systeme bedeutet das: „Security by Design“ wird gesetzlich verbindlich.

Die zentralen Anforderungen lauten:

– **Sichere Entwicklungsprozesse**
Der gesamte Hardwareentwicklungsprozess muss dokumentiert sicherheitsorientiert erfolgen – inklusive Threat Modeling, Risikobewertungen und ggf. Penetrationstests bereits im Prototypenstadium.

– **Physische Sicherheit**
Komponenten müssen gegen Manipulation gesichert sein, z.B. durch: Tamper Detection, geschützte Speicherbereiche (z.B. Secure Boot, TPM, HSM) und physische Zugriffskontrollen.

– **Sichere Schnittstellen**
Alle externen Ports und Interfaces (USB, Ethernet, PCIe etc.) müssen dokumentiert und kontrollierbar sein, gegen Missbrauch abgesichert werden und bei Bedarf deaktivierbar sein.

– **Sichere Auslieferung**
Vor Inverkehrbringen müssen Produkte einen Sicherheitscheck durchlaufen, der bekannte Schwachstellen ausschließt und einen sicheren Auslieferungszustand garantiert.

4.4 Anforderungen des CRA an Embedded Software

Der CRA verpflichtet Hersteller, Sicherheitsfunktionen konsequent und standardmäßig umzusetzen – von der Architektur bis zur Updatefähigkeit. Für Embedded-Software ergeben sich daraus folgende Kernanforderungen:

– **Security by Design & by Default**
Sicherheitsfunktionen müssen von Anfang an integriert und standardmäßig aktiviert sein. Werkseinstellungen dürfen keine Schwachstellen enthalten.

– **Vollständige Übersicht über Softwarekomponenten (SBoM)**
Alle eingesetzten Softwaremodule – inkl. Open-Source-Bibliotheken – müssen dokumentiert werden, um Transparenz und schnelle Reaktion auf Sicherheitslücken (z.B. CVEs) zu ermöglichen.

– **Langfristige Patch- & Updatefähigkeit**
Sicherheitsupdates müssen über den gesamten Supportzeitraum automatisiert und sicher durchführbar sein – z.B. per OTA (Over-the-Air).

– **Sichere Protokollierung**
Logging sicherheitsrelevanter Ereignisse muss Bestandteil der Software sein, inklusive Schutz der Protokolle gegen Manipulation.

– **Schnelle Reaktion auf Vorfälle**
Innerhalb von 24 h müssen Behörden über aktiv ausgenutzte Schwachstellen informiert werden, Nutzer spätestens nach 72 h.

GLOSSAR

„Safety. bzw. Funktionale Sicherheit“
Schutz von Mensch & Umwelt vor dem System

„Security“
Schutz des Systems vor dem Menschen

„Cybersicherheit“
Schutz des Systems, im speziellen vor Angriffen aus dem Internet.

„Schwachstelle“
Fehler im Design oder in der Umsetzung, die ein Angreifer ausnutzen könnte.

„Vorfall“
Von einem Angreifer ausgenutzte Schwachstelle in einem System mit negativen Auswirkungen.

„Bedrohung“
Potenzielles Szenario eines Vorfalls.

„Risiko“
Gemäß Eintrittswahrscheinlichkeit & Auswirkungen beurteilte Bedrohung mit einer daraus resultierenden Risikoeinschätzung.

„Schnittstelle“
Interface (logisch oder physisch), das für einen Angriff verwendet werden kann.

„Asset“
Schützenswerter Aspekt eines Systems (Programm, Konfiguration, Daten,...).

„Embedded System”
Ein spezialisiertes Computersystem, das fest in ein technisches Gerät integriert ist und dort eine klar definierte Funktion übernimmt.

“Embedded Linux”
Eine angepasste Version des Linux-Betriebssystems, die in Embedded Systemen eingesetzt wird, um komplexe Aufgaben wie Vernetzung, GUI oder Update-Management zu ermöglichen.

“Embedded Hardware”
Die für Embedded Systeme entwickelte oder angepasste Hardware, bestehend aus Prozessor, Speicher und Schnittstellen, optimiert für Stabilität, Energieeffizienz und Langlebigkeit.

“Microcontroller”
Eine kompakte Recheneinheit mit begrenzter Leistung, die Steuerungs- und Überwachungsaufgaben in Embedded Systemen zuverlässig übernimmt.

“Applikationsprozessor”
Ein leistungsfähiger Prozessor mit Unterstützung für Betriebssysteme wie Linux, der für grafikintensive, vernetzte oder rechenintensive Anwendungen in Embedded Devices verwendet wird.

„SBOM (Software Bill of Materials)“
Eine vollständige Auflistung aller enthaltenen Software-Komponenten eines Produkts, die Transparenz schafft und Sicherheits- sowie Compliance-Prüfungen ermöglicht.

ANHÄNGE

SOFTWARE BILLS OF MATERIALS (SBOM) & SCHWACHSTELLENMONITORING

Ein weiterer zentral geforderter Punkt im CRA ist die Erstellung einer Software-Stückliste, auch Software Bill of Materials (SBoM) genannt. Hierbei handelt es sich **um eine Liste, in der alle Bestandteile einer Software**, wie bspw. Bibliotheken, Module und andere Abhängigkeiten aufgeführt sind. Sie hilft dabei, einen klaren Überblick darüber zu bekommen, wie die Software aufgebaut ist und welche Komponenten verwendet werden. Moderne Softwareprojekte haben oft viele Abhängigkeiten, welche wiederum selbst Abhängigkeiten an weitere Pakete definieren, aber teils unterschiedliche Versionen fordern. Package-Manager helfen dabei, diese Abhängigkeiten aufzulösen und passende Versionen zu laden. Mithilfe einer SBoM kann anschließend festgehalten werden, welche Komponenten in welcher Version nun tatsächlich verwendet wurden.

Solche Stücklisten können automatisch mit Tools wie Syft erstellt werden. Diese Tools nutzen oftmals die Konfigurations- bzw. Lockfiles der Package Manager und sind somit ohne großen Aufwand in bestehende Build-Prozesse zu integrieren. Je nach Format können auch die Application-Packages selbst analysiert werden, wenn diese die notwendigen Metadaten enthalten, wie das zum Beispiel bei .jar-Files der Fall ist. Wenn man eingebettete Systeme entwickelt, kann man dafür auch Build-Werkzeuge wie Yocto nutzen und die damit erfassten Abhängigkeiten anschließend mit Programmen wie Dependency-Track oder Trivy überprüfen und verwalten.
Es bietet sich an, die Erstellung der SBoM in eine bestehende Build-Pipeline zu integrieren, somit kann diese ohne zusätzlichen manuellen Aufwand für jeden Build bzw. Release automatisch erstellt werden.

Die SBoM dient nicht nur zur Erfüllung der CRA-Anforderungen, sondern bietet auch einen praktischen Mehrwert im Softwareentwicklungsprozess. So ermöglicht es eine SBoM die Lizenzen der verwendeten Komponenten zu überprüfen, aber auch in Schwachstellendatenbanken nach bekannten Schwachstellen zu suchen. Diese Information kann genutzt werden, um die Auswirkungen auf das eigene Produkt zu analysieren und bei Bedarf Maßnahmen ergreifen zu können. Idealerweise ist dieses Schwachstellenmonitoring im Softwareentwicklungsprozess fest verankert.

Die Experten der Limes Security können bei der Definition eines solchen Prozesses beratend zur Seite stehen, bieten aber auch Trainings an, damit die handelnden Personen das notwendige Wissen erwerben können, um mit den vorhandenen Daten bestmöglich arbeiten zu können. Sollten Annahmen getroffen werden, dass z.B. bekannte Schwachstellen in verwendeten Komponenten keine Auswirkungen auf das eigene Produkt haben können, können diese in einem Penetration-Test durch erfahrene Tester der Limes Security unabhängig überprüft werden.

GELIN SBOM UND MONITORING AUS DER PRAXIS; SCREENSHOTS VON GELIN

In Abbildung 1 ist die Liste der Abhängigkeiten im build.gradle-File eines beispielhaften Java-Programms zu sehen. Diese Liste beinhaltet nur die vom Entwickler geforderten Abhängigkeiten, nicht aber deren Komponenten. Daher bietet diese Auflistung keinen vollständigen Überblick. Im Gegensatz dazu zeigt Abbildung 2 die gesamte Liste der verwendeten Komponenten und deren exakte Version, wie von einer SBoM zu erwarten ist. Diese Liste wurde mit Syft erstellt und kann zur weiteren maschinellen Verarbeitung auch in anderen Formaten wie SPDX oder CycloneDX generiert werden.

```
plugins {
        id 'java'
        id 'org.springframework.boot' version '3.5.1-SNAPSHOT'
        id 'io.spring.dependency-management' version '1.1.7'
}

group = 'com.example'
version = '0.0.1-SNAPSHOT'

java {
        toolchain {
                languageVersion = JavaLanguageVersion.of(21)
        }
}

repositories {
        mavenCentral()
        maven { url 'https://repo.spring.io/snapshot' }
}

dependencies {
        implementation 'org.springframework.boot:spring-boot-starter-data-jpa'
        implementation 'org.springframework.boot:spring-boot-starter-web'
        testImplementation 'org.springframework.boot:spring-boot-starter-test'
        testRuntimeOnly 'org.junit.platform:junit-platform-launcher'
```

```
}

tasks.named('test') {
        useJUnitPlatform()
}
```

Abbildung 1: Defintion der Abhängigkeiten eines Java-Programms

NAME	VERSION	TYPE
HikariCP	6.3.0	java-archive
angus-activation	2.0.2	java-archive
antlr4-runtime	4.13.0	java-archive
aspectjweaver	1.9.24	java-archive
byte-buddy	1.17.5	java-archive
classmate	1.7.0	java-archive
demo	0.0.1-SNAPSHOT	java-archive
hibernate-commons-annotations	7.0.3.Final	java-archive
hibernate-core	6.6.15.Final	java-archive
istack-commons-runtime	4.1.2	java-archive
jackson-annotations	2.19.0	java-archive
jackson-core	2.19.0	java-archive
jackson-databind	2.19.0	java-archive
jackson-datatype-jdk8	2.19.0	java-archive
jackson-datatype-jsr310	2.19.0	java-archive
jackson-module-parameter-names	2.19.0	java-archive
jakarta.activation-api	2.1.3	java-archive
jakarta.annotation-api	2.1.1	java-archive
jakarta.inject-api	2.0.1	java-archive
jakarta.persistence-api	3.1.0	java-archive
jakarta.transaction-api	2.0.1	java-archive
jakarta.xml.bind-api	4.0.2	java-archive
jandex	3.2.0	java-archive
jaxb-core	4.0.5	java-archive
jaxb-runtime	4.0.5	java-archive
jboss-logging	3.6.1.Final	java-archive
jul-to-slf4j	2.0.17	java-archive
log4j-api	2.24.3	java-archive
log4j-to-slf4j	2.24.3	java-archive
logback-classic	1.5.18	java-archive
logback-core	1.5.18	java-archive
micrometer-commons	1.15.0	java-archive
micrometer-observation	1.15.0	java-archive
slf4j-api	2.0.17	java-archive
snakeyaml	2.4	java-archive
spring-aop	6.2.7	java-archive
spring-aspects	6.2.7	java-archive
spring-beans	6.2.7	java-archive
spring-boot	3.5.1-SNAPSHOT	java-archive
spring-boot-autoconfigure	3.5.1-SNAPSHOT	java-archive

spring-boot-autoconfigure	3.5.1-SNAPSHOT	java-archive
spring-boot-jarmode-tools	3.5.1-SNAPSHOT	java-archive
spring-context	6.2.7	java-archive
spring-core	6.2.7	java-archive
spring-data-commons	3.5.0	java-archive
spring-data-jpa	3.5.0	java-archive
spring-expression	6.2.7	java-archive
spring-jcl	6.2.7	java-archive
spring-jdbc	6.2.7	java-archive
spring-orm	6.2.7	java-archive
spring-tx	6.2.7	java-archive
spring-web	6.2.7	java-archive
spring-webmvc	6.2.7	java-archive
tomcat-embed-core	10.1.41	java-archive
tomcat-embed-el	10.1.41	java-archive
tomcat-embed-websocket	10.1.41	java-archive
txw2	4.0.5	java-archive

Abbildung 2: Liste der tatsächlich verwendeten Komponenten des Java Programms

In Abbildung 3 ist ein das Monitoring Dashboard von OWASP Dependency Track zu sehen. Damit können die Inhalte der SBoMs dargestellt und deren Änderungen getrackt werden, um vulnerable und/oder veraltete Komponenten zu erkennen und deren Upgrades zu tracken.

Abbildung 3: Monitoring Dashboard von Dependency-Track

Mit der Verwendung der oben genannten Tools gelingt es einfach und schnell, eine SBoM ohne großen Aufwand zu generieren. Außerdem tätigt man damit erste Schritte in Richtung Konformität mit dem CRA. Aus genau diesem Grund ist es jedoch wichtig, Tools zu kennen und zu verwenden, auf die man sich verlassen kann.

VERWENDUNG VON BEREITS EXISTIERENDEN STANDARDS

Der CRA ist vorsätzlich sehr generisch formuliert worden, sodass das Inverkehrbringen von Produkten mit digitalen Elementen so einfach wie möglich ist. Dies erschwert es allerdings, konkrete Anweisungen und Richtlinien für die Konformität mit dem CRA zu definieren. Trotz dessen hat die ENISA für bereits bestehende Standards erörtert, wie gut sie die Anforderungen des CRA erfüllen und welche Lücken bei diesen noch bestehen.

Als sinnvolle Stütze zur Implementierung und Konformität mit dem Anhang 1 hat sie die Serie der IEC 62443 genannt, da die Standards 4-1 und 4-2 große Teile der Anforderungen des CRA abdecken.

HARMONISIERTE NORMEN

Harmonisierte Normen sind technische Spezifikationen, welchen von anerkannten europäischen Normungsorganisationen (z.B. CENELEC) im Auftrag der Europäischen Union erarbeitet und veröffentlicht werden mit dem Ziel, Vorgaben zur Erfüllung von Rechtsvorschiften zu definieren. Wenn die erarbeiteten Normen den Vorstellungen der EU-Kommission entsprechen, werden diese aufgenommen und als harmonisierte Norm geführt. Dadurch bieten sie Rechtssicherheit. Wenn ein Hersteller seine Konformitätsvermutung auf Basis der Norm(en) darlegen kann und die Anforderungen wie spezifiziert erfüllt sind, ist auch genug zur Erfüllung der Regularie umgesetzt worden. Für den CRA gibt es noch keine harmonisierten Normen. Arbeitsgruppen haben hier ihre Tätigkeit aufgenommen. Mit ersten Entwürfen ist im Jahr 2026 zu rechnen.

Internationale Normen wie die IEC 62443, speziell die für Hersteller relevanten Teile 4-1 (sichere Entwicklungsprozesse), bzw. 4-2 (technischen Security Anforderungen an Komponenten), sind keine harmonisierten Normen und können es auch künftig nicht werden. Eine Zertifizierung nach den Normen bietet also auch keine Rechtssicherheit, ausreichend für den CRA getan zu haben. Trotzdem ist in Abwesenheit von harmonisierten Normen eine international anerkannte und bewährte Standardreihe wie die IEC 62443 definitiv ein guter Startpunkt. Viele der Anforderungen werden in ähnlicher Form zu erwarten bzw. umzusetzen sein. Um einen Eindruck zu bekommen, wie eine harmonisierte Norm aufgebaut sein kann, empfiehlt sich ein Blick in die EN 18031 Reihe. Diese definiert Vorgaben zur Erfüllung der Cybersicherheitsanforderungen aus der Funkanlagenrichtlinie. Die EN 18031 ist nicht als harmonisierte Norm für den CRA gelistet und bietet daher auch keine Rechtsicherheit.

Als erste harmonisierte Norm, die die Cybersecurity Anforderungen definiert, ist sie ein guter Richtwert dafür, was erwartet werden kann.

Einige der Anforderungen werden sich wahrscheinlich in leicht abgeänderter Version in einer Norm für den CRA wiederfinden. Im Folgenden findet sich eine Gegenüberstellung, in der inhaltlich die Anforderungen des CRA mit den technischen Anforderungen der EN 18031 verknüpft werden.

CRA Anforderung	Passende EN18031 Anforderungen	Kommentar
2a	GEC-1	
2b		
2c	SUM-1, SUM-2, SUM-3	
2d	ACM-1, ACM-2, AUM-1, AUM-2	
2e	SSM-1, SSM-3, SCM-1, SCM-3	
2f	SSM-1, SSM-2, SCM-1, SCM-2	Meldung von Beschädigung wird nicht erwähnt.
2g		
2h	NMM-1, TCM-1	
2i	GEC-2	Wahrscheinlich nicht ausreichend, aber hilfreich.
2j	GEC-2, GEC-3, GEC-5	
2k		
2l	LGM-1 (18031-2)	Nur Aufzeichnung wird erwähnt, Opt-Out fehlt ebenso.
2m	DLM-1 (18031-2)	Nur anwendbar auf Daten und Einstellungen.

IEC 62443:

In der Einleitung zu diesem Kapitel wurde bereits erwähnt, dass die ENISA die Normen IEC 62443-4-1 und -4-2 analysiert hat und dabei feststellte, dass diese Standards eine solide Grundlage für den Cyber Resilience Act bilden. Wir geben in folgender Tabelle unsere Einschätzung zu diesem Statement ab. Hier ist jedoch Vorsicht geboten: Weder die Aussage der ENISA noch die Einschätzung der Experten bei Limes Security bieten rechtliche Sicherheit im Falle einer Konformitätsprüfung!

Da den CRA keine harmonisierten Standards betreffen und Implementierungs-richtlinien von der EU noch folgen sollten, gibt es noch keine Sicherheit auf Konformität in Bezug auf existierende Standards wie der IEC 62443. Dennoch bietet sie eine gute Grundlage, um sich mit der Cybersicherheit eines Produkts zu befassen und erste Meilensteine auf dem Weg zur Konformität zu legen. Die folgende Tabelle soll zeigen, wie Limes Security die IEC 62443 hinsichtlich des CRA bewertet:

ANFORDERUNG	PASSENDE 62443 ANFORDERUNGEN	KOMMENTAR
Anhang | Teil |		
2a	SM-11, SM-12	
2b	SD-4, FR-7: CR7.7	
2c	SUM-4, FR-3: CR3.10	
2d	FR-1, FR-2	
2e	FR-4	
2f	SM-6, FR-3	Relevante erhaltene Daten, Meldung wird nicht angesprochen
2g		
2h	FR-7: CR7.1, CR7.2	
2i	FR-5: CR5.1	
2j	SD-4, FR-3: CR3.11, FR-7: CR7.6, CR7.7	
2k	SD-4	
2l	FR-6, FR-2: CR2.8, CR2.11, CR2.12	Opt-Out wird nicht erwähnt
2m	SR-3	

ANFORDERUNG	PASSENDE 62443 ANFORDERUNGEN	KOMMENTAR
Anhang | Teil ||		
Abs. 1	SVV-3, DM-1	
Abs. 2	SM-11, DM-4, SUM-1, SUM-5	
Abs. 3	SVV	
Abs. 4	DM-3, DM-5, SUM-2	DM-3 für Dokumentation, DM-5 für Offenlegung
Abs. 5	DM-5	
Abs. 6	DM-1	
Abs. 7	SUM-4	Automatische Updates werden nicht erwähnt.
Abs. 8	SUM-5, DM-5	
Anhang ||		
Abs. 1		
Abs. 2	DM-1	
Abs. 3		
Abs. 4	SR-1	
Abs. 5	SR-1, SR-2	
Abs. 6		
Abs. 7		
Abs. 8		
8a	SG-1, SG-3, SG-5	
8b	SG-3	
8c	SG-3, DM-5	
8d	SG-4	
8e	DM5	
8f	SG-1, SG-2, SG-3, SG-4, SG_5, SG-6	
Abs. 9		

START YOUR SECURITY JOURNEY.

Limes Security GmbH – Softwarepark 49 – 4232 Hagenberg im Mühlkreis – **www.limessecurity.com**

Ginzinger electronic systems GmbH – Gewerbegebiet Pirath 16 – 4952 Weng im Innkreis – **www.ginzinger.com**