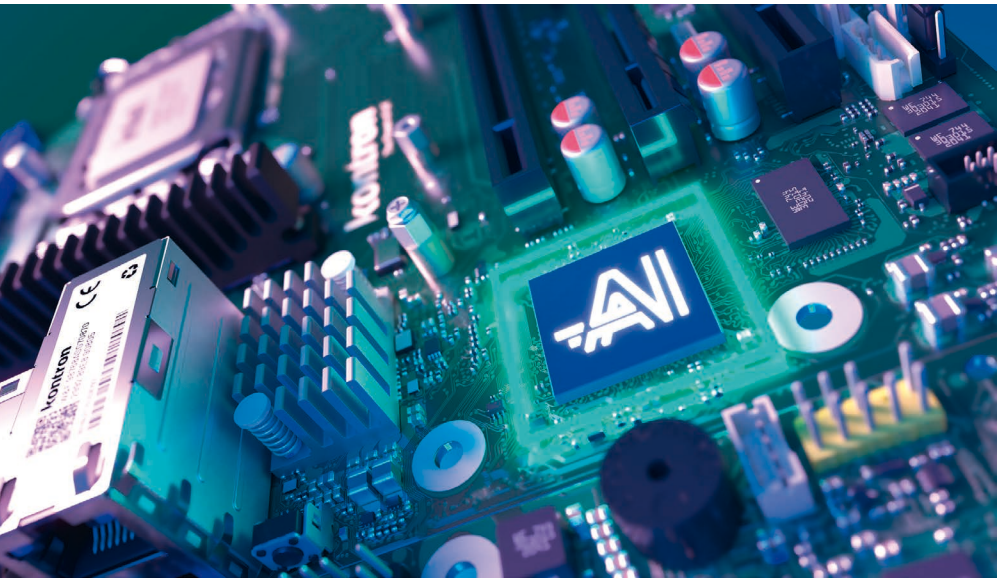
CRA-Compliance in der Praxis: So gelingt der Weg zur Cyberresilienz



Viele Unternehmen haben sich noch nicht ausreichend auf die Veränderungen eingestellt, die der Cyber Resilience Act (CRA) ab Ende 2027 bringt. Software-Entwicklungsprozesse werden formaler, die Dokumentation auch im Open-Source-Umfeld anspruchsvoller. Besonders die geforderte Update-Fähigkeit stellt viele Hersteller vor Herausforderungen. „CRA-ready" Betriebssysteme und Komponenten können den Weg zur Compliance erheblich verkürzen.

Schaden abwenden

Der Cyber Resilience Act soll angesichts der zugespitzten Lage im Bereich Cybersicherheit dazu beitragen, Schaden von Europa abzuwenden. Ziel der EU-Gesetzgebung ist ein höheres Cybersecurity-Schutzniveau für vernetzte Produkte. Dafür muss die Sicherheit – auch für Produkte, die schon länger auf dem Markt sind – systematisch durch Maßnahmen wie die Verankerung von Security im Produktdesign, Update-Fähigkeit und das wirksame Schließen von Schwachstellen erhöht werden.

Jetzt Prioritäten setzen

Unternehmen müssen alle in den Verkehr gebrachten Produkte ab dem Stichtag 11.12.2027 entsprechend zertifiziert haben, um (weiter) das CE-Kennzeichen tragen zu dürfen. Die Einhaltung des CRA hat damit einen starken Einfluss auf die Wettbewerbsfähigkeit, doch viele Unternehmen machen sich das noch nicht ausreichend bewusst. Es funktioniert nicht mehr, das Thema an die eigenen Lieferanten weiterzureichen, denn derjenige, der das Produkt in Verkehr bringt, haftet für das Gesamtsystem. Anders als die im letzten Jahr in Kraft getretene NIS-2-Richtlinie ist der CRA ein Regelwerk, das auch sehr konkrete, detaillierte technische Anforderungen an Anlagen und Komponenten mit sich bringt. Die EU gibt dazu eine Reihe von Normen heraus, von denen ein Teil noch nicht letztgültig ausdefiniert ist. Dennoch drängt die Zeit, wenn ab 2027 jedes ausgelieferte System die neue Norm erfüllen soll.

Notwendige Anpassungen

Der CRA erfordert aufwendige organisatorische Anpassungen. Der CRA bildet mit der EN 40000-Reihe die Blaupause für industrielle Cybersecurity. Bereits bestehende, aber nicht verpflichtende Normen, wie die IEC 62443-4-1 und IEC 62443-4-2, gehen darin auf. Unternehmen, die bereits die IEC 62443 anwenden, sind gut auf den CRA vorbereitet. Bereits gültige Normen, wie etwa die EN 18031, die Teil der Radio Equipment Directive (RED) ist, werden übernommen bzw. durch den CRA verbindlich für alle Gerätetypen abgelöst. Wer heute noch nicht mit der IEC 62443 oder RED vertraut ist, muss jetzt beginnen, sich damit zu beschäftigen: Ein rascher Einstieg ist unabdingbar.

CRA-Regelkonformität

Je nachdem, nach welcher Sicherheitsklasse das Produkt gelistet ist, muss eine Prüforganisation wie etwa der TÜV die Lösung prüfen. Das bedeutet häufig einen immensen Mehraufwand. Zugleich ist davon auszugehen, dass sich die Standardisierung durchsetzen wird – und bei Ausschreibungen bald die CRA-Regelkonformität eingefordert wird. Für international agierende Unternehmen, die den europäischen Markt bedienen, bedeutet das in aller Regel, dass sie

Autor:
Stefan Eberhardt
Senior Business Developer IoT Software und CRA-Experte
Kontron Europe GmbH
www.kontron.com/de

die Thematik für ihre jeweiligen Lösungen gleich für alle Märkte adressieren. Zunächst geht es vor allem darum, ein Verständnis für die Risikoeinschätzung zu entwickeln, daraus technische Maßnahmen für das Produkt abzuleiten und die eigenen Lieferanten einzubeziehen.

Der Weg ist teils holprig

Die Normen sind harmonisiert und finden sich in unterschiedlichen Regelwerken wieder. Für diejenigen Unternehmen, die in der Vergangenheit schon an Normen wie zum Beispiel der EN 18031 (die RED-Cyberanforderungen konkretisiert) mitgearbeitet haben, ist der nächste Schritt nicht ganz so groß. Zugleich ist deutlich, dass sich etwa im Maschinen- und Anlagenbau bei weitem noch nicht alle Unternehmen auf den Weg gemacht haben. Für sie wird es deutlich schwieriger, denn während bisher bei der CE-Zertifizierung in der Selbstdeklaration noch Spielraum bestand, verändern sich die Anforderungen mit dem CRA erheblich.

Software Bill of Materials

Es gibt auch noch einige Unwägbarkeiten. In vielen Produkten ist Standard-Software wie etwa Windows von Microsoft als Teilkomponente verbaut. Die seit 01.08.2025 in Kraft getretene Erweiterung der RED-Direktive, die EN 18031, führt hier zu einem Dilemma: Zur nun geforderten SBOM (Software Bill of Materials) würde auch eine entsprechende Offenlegung zu Windows gehören. Die SBOM trägt dazu bei, dass sich schnell identifizieren lässt, ob das eigene System betroffen ist, sobald eine neue Schwachstelle publik wird. Es gibt jedoch derzeit keine RED-spezifische Konformitätserklärung von Microsoft, die von einem Prüflabor akzeptiert wird. Den Herstellern fehlt damit eine wichtige Bestätigung für ihr Produkt. Hier wird die Zukunft zeigen, wie sich diese Herausforderung lösen lässt.

Neue Anforderungen für Embedded Hard- und Software

Zum einen werden architektonische Aspekte eingefordert wie ein Sicherheitsanker im Produkt: Eine Hardware Root of Security/Trust bedeutet, dass ein System vor dem Start überprüfen können muss, ob Bootloader, Firmware und Betriebssystem genau in der für das Produkt vorgesehenen Version vorliegen und nicht manipuliert oder verändert wurden. Dadurch ist es künftig nicht mehr möglich, Software oder zusätzliche Programme „einfach nachträglich aufzusetzen“, um die Lauffähigkeit sicherzustellen: Jede Änderung muss in das Sicherheitskonzept integriert und freigegeben werden. Teilweise werden Updates von Herstellern noch als Link auf der Homepage zur Verfügung gestellt und die Kunden per E-Mail darüber informiert. Nun muss das System also selbst „verstehen“, dass ein Software-Update passt und nicht manipuliert wurde.

Kontinuierliches Schwachstellen-Monitoring

Das neue Gesetz verlangt darüber hinaus ein kontinuierliches Schwachstellen-Monitoring und einen Überblick über potenzielle Risiken, die in Zwischenkomponenten oder im Zusammenspiel von Komponenten im Gesamtsystem entstehen können. Die Frequenz von Updates und Releases ist je nach Security-Klassifizierung des Produkts zu wählen. Für Standardprodukte ist das typischerweise einmal monatlich. Gerade bei älteren Produkten ist die Update-Thematik komplex.

Der Software-Entwicklungsprozess verändert sich

Die größte Umstellung für die Unternehmen liegt sicherlich darin, dass die gewohnten Pfade verlassen werden müssen und die bisherige Flexibilität in der Produktentwicklung zum Teil verlorengeht. Bisher wurden beispielsweise Open-Source-Produkte ohne viel organisatorischen Overhead genutzt. Jetzt gilt es, Listen vorzuhalten, welche Lizenzen es gibt und welche Komponenten genutzt werden. Diese Dokumente müssen gemeinsam mit dem Produkt herausgegeben werden. Die Open-Source-Community arbeitet aktiv an Unterstützung, damit im kommerziellen Umfeld mit den CRA-Anforderungen umgegangen und gleichzeitig weiter auf die offene Entwicklung gesetzt werden kann.

Generell lässt sich sagen: Die Software-Entwicklung wird deutlich formaler und es gelten klare Regeln für einen sicheren Development-Prozess. Nun ist mehr Dokumentation im Vorfeld, bessere Produktplanung und der Nachweis notwendig, dass „secure by design“ konzipiert und entwickelt wurde. Die Lösungen müssen also dezidiert gebaut und über den Lebenszyklus gewartet werden.

Sicherheitskonzept erfüllen

Wie bisher bei Problemen eine schnelle „Umgehung“ zu bauen und einfach über Nacht rasch ein Release oder ein Update zu veröffentlichen, ist im Kontext des CRA schlicht nicht mehr möglich. Zu prüfen ist nun auch, ob externe Entwickler oder Entwicklungsteams, die nicht nach CRA-Vorgaben arbeiten, z. B. in Ländern außerhalb der EU, ebenfalls im Sicherheitskonzept abgedeckt

sind. Hier sind definierte Schnittstellen notwendig. Auch Schulungen bekommen noch einmal einen höheren Stellenwert. Die Ansprüche an das Testing verändern sich ebenfalls. Zum Teil müssen unterschiedliche Personen Funktionen testen, was gegebenenfalls größere Teams erfordert. In der Folge wird es deutlich weniger kleine Standardprogramme oder Kleinserien geben. Die kleinen, schnellen Projekte für Ad-hoc-Lösungen werden weniger – stattdessen muss gleich strategischer und über den Einzelfall hinaus gedacht werden. Damit verändert sich gegebenenfalls auch die Produktpalette.

Wie sich das Sicherheits-Level schnell anheben lässt

CRA-vorzertifizierte Produkte mit den entsprechenden Nachweisen können ein wichtiger Schlüssel sein, um nun schneller in die Umsetzung zu kommen. Insbesondere im Embedded-Linux-Umfeld steigt der Druck zu mehr Professionalität und damit der Bedarf an vorkonfigurierten und nachweisbaren Security-Bausteinen. Hier können „CRA-ready“ Plattformen zentrale Funktionen wie Secure Boot, sichere Update-Mechanismen (Over the Air, OTA), SBOM und Nachweisdokumentation auf Basis des Board Support Package (BSP) sicher bereitstellen. Ein solches vorzertifiziertes, normkonformes Embedded-Linux reduziert sowohl den Entwicklungsaufwand des Unternehmens als auch die Risiko- und Audit-Komplexität erheblich. In der Praxis zeigt sich bereits deutlich, dass Beratungs- und Software-Dienstleistungen in diesem Umfeld stärker nachgefragt werden. Was früher zumeist der kritischen Infrastruktur vorbehalten war, findet jetzt im Standard Einzug.

Firewalls

Ein weiterer Ansatzpunkt – nicht zuletzt für bestehende Produkte im Praxiseinsatz – sind Firewalls, die als Sicherheits-Gateway zwischen Netzwerk und Endsystem zum Einsatz kommen. Anders als bei der klassischen „Deep Packet Inspection“ reduziert sich der administrative Aufwand, da keine aufwändige Verteilung und Pflege von Zertifikaten in allen Systemen mehr notwendig ist. Die KI prüft direkt auf potenziell schädliche Datenpakete. Die Firewall kann als Teil des Gesamtsystems vorgeschaltet werden. Damit lassen sich viele Probleme mit nicht mehr updatefähigen Systemen lösen, die dann wieder normkonform im Rahmen des Netzwerks betrieben werden können. Der Verbund aus Bestandsystem und Firewall Appliance wird hier als ein Gesamtsystem betrachtet, in dem intern nur definierte Services geteilt werden. Etwa bei Medizintechnik wie Computertomografen im Krankenhaus, Cash-Handling-Systemen im Bank- und Retailbereich oder Fahrkartenlesegeräten im öffentlichen Nahverkehr.

Painpoint: Update-Fähigkeit über den Lebenszyklus

Hersteller verpflichten sich im CRA, Schwachstellen über den Lebenszyklus ihrer Produkte zu tracken und zu beseitigen. Ohne Update-Fähigkeit lässt sich diese Basisanforderung nicht erfüllen. Die Vorgaben sehen vor, dass Security-Updates mindestens fünf Jahre nach Auslieferung gewährleistet sein müssen. Viele Anwender nutzen Systeme jedoch über 10 bis 20 Jahre. Embedded-Hersteller mit eigenem Betriebssystem können kontinuierliche Updates zwar leicht selbst liefern. Bei BIOS, Firmware und hardware-nahen Komponenten besteht dennoch eine Abhängigkeit von Zulieferern wie AMI oder Intel: Endet der Support, endet letztlich auch die Updatefähigkeit des Gesamtsystems. Diese Herausforderung lässt sich jedoch durch kundenindividuelle Absprachen zu kostenpflichtigem Extended Support oder durch andere Ansätze lösen, wenn Updates nicht mehr möglich sind.

Der Schutzbedarf steigt

Anders als bei Smartphone-Updates sind Updates im industriellen Umfeld deutlich komplexer. Maschinen und Anlagen bestehen häufig aus Komponenten mehrerer Hersteller, Integratoren und Softwarelieferanten. Zwar kann ein Hersteller Updates zur Verfügung stellen, doch nachgelagerte Partner und Betreiber müssen die Softwarepakete jeweils prüfen, gegebenenfalls adaptieren und in ihrer jeweiligen Umgebung freigeben.

Hier kommt noch viel Untersuchungs- und Evaluierungsaufwand auf die Lieferanten und Kunden zu, um letztlich sicherzustellen, dass gesetzliche Vorgaben eingehalten werden können. Aufgrund der erforderlichen Prozess- und Organisationsveränderungen ist es wichtig, dass sich alle betroffenen Unternehmen jetzt auf den Weg machen. Im letzten Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) wurden bis Mitte 2025 pro Tag 119 neue Schwachstellen gefunden – das waren 25 Prozent mehr als im Vorjahr. Höchste Zeit also für ein höheres Schutzniveau, von dem Wirtschaft und Gesellschaft in Europa profitieren. ◄