

Verschiedene Wege zu Cybersicherheit gemäß CRA

von Oliver Roth



Bild: Oryferry/stock.adobe.com Generiert mit KI

Wer zu spät kommt, den bestraft der Cyber Resilience Act spätestens am 11. Dezember 2027: Dann dürfen nur noch Produkte mit digitalen Elementen ein CE-Kennzeichen tragen und in Verkehr gebracht werden, die den Vorgaben des CRA entsprechen. Infrage kommen individuelle Neu- und Weiterentwicklungen oder der Wechsel zu Standardkomponenten. Beide Strategien haben ihre Berechtigung, Abwarten ist jedoch keine Option.

Ab dem 11. Dezember 2027 dürfen nur noch Produkte mit digitalen Elementen in Verkehr gebracht werden, die den Vorgaben des CRA entsprechen. Bereits am 20. Januar 2027 löst zudem die Maschinenverordnung die Maschinenrichtlinie ab und verlangt unter anderem einen Manipulationsschutz für Software und Daten mit Sicherheitsfunktionen.

Bereits verstrichen: der erste Stichtag

Ein weiterer Termin ist kürzlich weitgehend unbemerkt verstrichen: Seit dem 11. September 2026 müssen Hersteller für Produkte, die bereits auf dem Markt sind, aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle melden – binnen 24 Stunden als Frühwarnung und binnen 72 Stunden als Meldung, innerhalb von längstens einem Monat als Abschlussbericht. Das setzt voraus, was formal erst später verlangt wird: eine Software-Stückliste, ein aktives Schwachstellen-Monitoring über alle verbauten Komponenten und eine handlungsfähige Instanz im Unternehmen.

Auf künftige Terminverschiebungen, Übergangsfristen oder andere Erleichterungen zu hoffen, ist daher keine tragfähige Strategie. Stattdessen sollte die Vorbereitung längst mit einer Risiko- und Bedrohungsanalyse begonnen haben. Deren Ergebnis dürfte in vielen Fällen sein, dass die in Maschinen und Anlagen verwendeten digitalen Komponenten für Steuerung, Kommunikation, Visualisierung und Bedienung weitgehend neu entwickelt oder ersetzt werden müssen. Damit stellt sich für Maschinenbauer und Industrieausrüster eine grundsätzliche Frage: Soll man Individuallösungen „sicher“ entwickeln (lassen) oder sichere Standardlösungen am Markt einkaufen und gegebenenfalls anpassen? Bevor diese Entscheidung getroffen wird, lohnt sich die Beschäftigung mit einer weiteren Frage, die der CRA aufwirft.

Der Name ist entscheidend

Schließlich erlegt die Verordnung demjenigen Pflichten auf, der ein Produkt mit digitalen Elementen unter eigenem Namen anbietet. Für die Maschine selbst ist das immer der



Web-Tipp

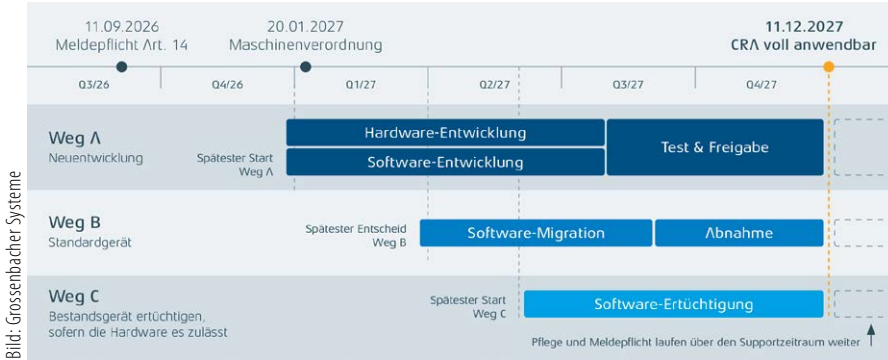
Lesen Sie alle Teile der Serie „CRA-Compliance in der Praxis“:

• Teil 1: Der „CRA-Day“ naht – sind Sie vorbereitet?

<https://bit.ly/3UUPj72>

• Teil 2: Warum CRA und Dev-SecOps zusammengehören –

<https://bit.ly/3V8tMrx>



Drei mögliche Wege zur
CRA-Compliance.

Maschinenbauer. Für das zugehörige Bediengerät hängt es davon ab, wessen Namen es trägt.

Wer ein Standardgerät einkauft und kenntlich macht, trägt diese Pflichten für das Gerät also nicht selbst. Der Gerätehersteller führt die Software-Stückliste, beobachtet Schwachstellen, stellt Updates bereit und meldet Vorkommnisse. Wer ein Gerät für sich entwickeln lässt und unter eigenem Label verbaut, wird selbst zum Hersteller (Inverkehrbringer) und übernimmt auch dessen Pflichten.

Dies gilt über den gesamten zugesagten Supportzeitraum, der nach dem CRA mindestens fünf Jahre beträgt, aber auch fünfzehn oder zwanzig Jahre dauern kann. Unabhängig davon bleibt der Maschinenbauer für die Maschine und die Software, die er darauf betreibt, verantwortlich.

Gründe für Individualentwicklungen

Kundenspezifische Geräte entstehen in der Regel nicht aus dem Wunsch, das Rad neu zu erfinden. Sie werden interessant, wenn Standardkomponenten wesentliche Anforderungen nicht erfüllen. Diese Anforderungen lassen sich im Wesentlichen in fünf Kategorien einteilen.

Die erste Kategorie betrifft mechanische Aspekte, etwa den Aufbau der Anlagen und deren Platzverhältnisse. Maschinenbauer müssen digitale Komponenten häufig in spezifische Einbausituationen einpassen. Knapper verfügbarer Raum,

besondere Geometrien, definierte Anschlusssituationen oder Anforderungen an Montage und Verkabelung können dazu führen, dass Standardgeräte nicht passen.

Die zweite Kategorie betrifft spezifische Sensorik und Aktorik. Ist sie erforderlich, kann eine maßgeschneiderte Steuerung Vorteile bieten. Schnittstellen, Signalaufbereitung, Messbereiche oder spezielle Echtzeitanforderungen lassen sich dann direkt in die Hard- und Softwarearchitektur integrieren.

Ein weiterer Faktor ist der Kostendruck. Nicht immer ist die Entwicklung individueller Elektronik teurer als der Kauf eines Serienprodukts, insbesondere dann, wenn dieses Funktionen mitbringt, die nicht benötigt werden. Dafür bedarf es jedoch größerer Stückzahlen, um Entwicklungsaufwand sowie Werkzeug- und Zertifizierungskosten zu amortisieren.

Der CRA verändert diese Rechnung, weil er Kosten für die laufende Pflege verursacht, die nicht von der Stückzahl abhängig sind, sondern pro Produkt anfallen. Dazu zählen der Aufwand für Software-Stücklisten, Schwachstellenbeobachtung, Patch-Bereitstellung, Regressionstests und Reaktionsfähigkeit. Bei einem Gerät auf einer offenen Plattform verteilt sich der Aufwand zudem auf mehrere Ebenen: Die zugrunde liegende Linux-Distribution wird vom Herausgeber gepflegt, das konkret installierte Betriebssystem vom Plattformanbieter, das Gerät vom Hersteller und die Applikation vom Maschinenbauer. Wer ein eigenes Linux-basiertes Gerät entwickeln lässt, verantwortet drei dieser Ebenen allein.

Die vierte Kategorie betrifft Differenzierung und Usability. Bedienkonzept, Gehäuse, Display, Bedienelemente und die gesamte User Experience können ein selbst entwickeltes HMI oder Bediengerät zum „Selling Point“ einer Maschine machen. Eine fünfte und letzte Kategorie ist unabhängig vom CRA – und oft entscheidend. Wo besondere regulatorische oder umgebungsbedingte Anforderungen gelten, etwa Explosionsschutz, erweiterte Temperaturbereiche oder die Nähe zur Medizintechnik, sind Standardprodukte schlicht keine Option. Ein Blick auf diese Anforderungen zeigt, dass kundenspezifische Entwicklung nach wie vor die richtige Strategie sein kann. Allerdings muss der externe Entwickler vor dem Hintergrund des CRA „Security by Design“ sowie eine langfristige Produktpflege mit sicheren Update- und Deployment-Prozessen beherrschen und Serienproduktion und Ersatzteilversorgung zuverlässig gewährleisten.

Gründe für Standardprodukte

Die Anforderungen des CRA dürften jedoch nur ein Grund sein, warum Grossenbacher Systeme als Individualentwickler seit einiger Zeit ein steigendes Interesse an regulatorisch abgesicherten Standardplattformen beobachtet. Das gilt vor allem, wenn diese Produkte eine offene Betriebssystemarchitektur und ein dynamisch wachsendes App-Ökosystem bieten.

Beides trifft exemplarisch auf das Ecosystem ‚ctrlX OS‘ von Bosch Rexroth zu und war Anlass zur Gründung der Grossenbacher Automation AG, die Standardprodukte auf Basis von ctrlX OS entwickelt und vertreibt.

Die Anforderungen an mechanische Integration und spezifische Schnittstellen können Maschinenbauer zudem häufig

neu bewerten. Muss sich das Bediengerät tatsächlich exakt an die vorgegebene Geometrie anpassen? Sind spezielle Ein- und Ausgänge zwingend erforderlich? Werden solche Anforderungen gelockert, werden moderne Standardkomponenten zu einer Option, vor allem, wenn sie Flexibilität durch Software und offene Architekturen bieten. Ein Beispiel hierfür sind Systeme, die Steuerung, Visualisierung und Bedienung in einem einzigen kompakten Gerät kombinieren, etwa ein „HMI-PLC all-in-one, powered by ctrlX OS“. Gerade für Low- und Mid-Complexity-Anwendungen in der Industrieautomation kann ein solches Gerät Vorteile bieten. Entscheidend sind dabei nicht allein die Hardware, sondern auch das Verhältnis von Performance, Kosten und Software-Flexibilität. „ctrlX OS“ basiert auf einer offenen Architektur und nutzt die Snap- und Container-Architektur von Ubuntu Core. Sie ermöglicht Python-basierte Anwendungen jenseits klassischer Soft-SPS und Visualisierung. Neue Funktionen lassen sich damit über Software ergänzen, etwa mit Python oder Low-Code, ohne Änderungen an der Hardwarearchitektur. Noch interessanter wird dieser Ansatz, wenn vorhandene Software weiter genutzt werden kann. Viele Maschinenbauer verwenden über Jahre entwickelte C- oder C++-Programme, die einen erheblichen Teil des eigenen Know-hows enthalten. Eine komplette Neuprogrammierung wäre technisch komplex und wirtschaftlich fragwürdig. Eine Alternative besteht darin, wertvolle „Legacy-Software“ containerisiert in ctrlX OS zu integrieren und schrittweise zu migrieren.

Schließlich gewinnt angesichts von CRA und Digitalisierung auch der Faktor Zeit an Bedeutung: Individualentwicklungen benötigen typischerweise mehrere Entwicklungsphasen – von der Spezifikation über Hardware- und Softwareentwicklung bis zu Tests, Validierung, Zertifizierung und Serienanlauf. Ein Standardprodukt kann diese Prozesse verkürzen.

Optionen sorgfältig prüfen

Zwischen Individualentwicklung und Standardkomponenten liegt eine dritte Möglichkeit, die häufig übersehen wird: der Einsatz von Serienprodukten, die über Software individualisiert werden. Der Gerätehersteller bleibt Inverkehrbringer des Geräts und trägt dessen Pflichten. Der Maschinenbauer bringt sein Know-how als Applikation, Visualisierung oder containerisierte Bestandssoftware ein und differenziert sich dort, wo dies sinnvoll ist.

Erst wenn spezifische Ein- und Ausgänge oder eigene Messtechnik unverzichtbar sind, kommt eine ergänzende kundenspezifische Baugruppe hinzu – als Zusatz zum Seriengerät, nicht als komplette Eigenentwicklung.

Es kommt also auf das einzelne Produkt an, das für den CRA vorbereitet werden soll. Kundenspezifische Lösungen haben auch in Zukunft ebenso ihre Berechtigung wie moderne Standardlösungen. Maschinenbauer und Industrieausrüster sollten die verschiedenen Optionen deshalb anhand ihrer konkreten Anforderungen prüfen. Dabei kann es hilfreich sein, wenn Anbieter wie die beiden Grossenbacher-Unternehmen verschiedene Optionen abbilden können, ohne die übergeordnete Perspektive aufzugeben.

ag



Oliver Roth

ist CEO von Grossenbacher Systeme und der Amalthea Gruppe.