Bild: © Frank H./stock.adobe.com

INDUSTRIE IM SICHERHEITS-CHECK: Der CRA und seine Folgen

In einer zunehmend vernetzten Welt, in der Cyberangriffe immer raffinierter werden, setzt die neue EU-Verordnung Cyber Resilience Act (CRA) neue Maßstäbe für die Cybersicherheit von Produkten mit digitalen Elementen – über ihren gesamten Lebenszyklus. Ziel ist es, Sicherheitsrisiken frühzeitig zu minimieren und verbindliche Anforderungen für Hersteller, Integratoren und Betreiber festzulegen. Besonders betroffen sind Unternehmen der Automatisierungs- und Fertigungsindustrie, da deren Systeme zunehmend vernetzt und softwaregesteuert sind. Doch was bedeutet der CRA konkret für die Branche? Um die Auswirkungen näher zu beleuchten, hat die Redaktion des SPS-MAGAZINs Security-Spezialisten einiger Unternehmen befragt.

INES STOTZ
Leitende Redakteurin

Wie bewerten Sie die Bedeutung des Cyber Resilience Act für die Automatisierungsbranche? Welche Chancen ergeben sich gegebenenfalls, welche Herausforderungen entstehen bei der Umsetzung? Und welche Rolle spielt ‚Usable Security'?

SIMON GÖGGEL, ADS-TEC: Der Cyber Resilience Act ist ein wichtiger Schritt zur Verbesserung der IT-Sicherheit in der Automatisierungsbranche. Er stellt sicher, dass Sicherheitsaspekte von Anfang an in die Entwicklung digitaler Produkte integriert werden. Für Unternehmen bietet das Gesetz eine große Chance: Durch höhere Sicherheitsstandards können sie das Vertrauen der Kunden stärken und sich Wettbewerbsvorteile sichern. Wer frühzeitig in Cybersecurity investiert, wird langfristig am Markt bestehen. Die größte Herausforderung liegt in der Umsetzung der strengen Anforderungen – insbesondere für kleinere Betriebe, die mit hohem finanziellen und personellen Mehraufwand rechnen müssen. Eine Schlüsselrolle spielt dabei Usable Security: Sicherheitslösungen müssen nicht nur robust, sondern auch benutzerfreundlich sein. Komplexe Authentifizierungsprozesse oder unklare Warnmeldungen führen dazu, dass Schutzmaßnahmen umgangen werden. Deshalb müssen Sicherheitsmechanismen intuitiv sein und sich nahtlos in den Arbeitsalltag integrieren.

FRANK BEHNKE, HILSCHER: Der CRA, die NIS2-Richtlinie und das NIS2UmsuCG haben eine enorme Bedeutung für

In Ausgabe 5 folgt Teil 2 unserer Umfrage zum Cyber Resilience Act. Dort geht es u.a. um den Aufwand der für die Umsetzung des CRA zu erwarten ist, um die Wettbewerbsfähigkeit und die wichtigsten Maßnahmen, die jetzt ergriffen werden sollten.

die Automatisierungsbranche. Neben strikteren Sicherheitsanforderungen kommen Haftungsfragen und die Pflicht zu regelmäßigen Sicherheitsupdates hinzu. Künftig wird es kein sicheres industrielles Netzwerk ohne tief integrierte Cybersecurity mehr geben. Die Chancen liegen in einer einheitlichen Regulierung und mehr Vertrauen in sichere Produkte. Unternehmen, die frühzeitig auf Security-by-Design und auf Standards wie IEC62443 setzen, können sich als verlässliche Partner im Markt positionieren. Die größte Herausforderung ist die praxisnahe Umsetzung. Viele Unternehmen unterschätzen noch die Tragweite der bevorstehenden Veränderungen. Unser Ziel ist es, hier mit Expertise zu unterstützen. Usable Security spielt dabei eine entscheidende Rolle. Sicherheitsmechanismen müssen anwenderfreundlich und effizient sein. Die beste Sicherheit hilft nichts, wenn sie schwer zu implementieren ist oder im Arbeitsalltag umgangen wird. Besonders Systeme mit zentralem Patch-Management bieten hier einen Wettbewerbsvorteil, da sie Sicherheitsupdates automatisieren und den Verwaltungsaufwand reduzieren.

Die größte Herausforderung ist die praxisnahe Umsetzung.

Frank Behnke,
Hilscher

THILO DÖRING, HMS: Der CRA ist ein bedeutender Meilenstein für die Automatisierungsbranche, da er darauf abzielt, die Cybersicherheit auf europäischer Ebene zu stärken. Die Umsetzung ist verpflichtend und die Umsetzungsfrist läuft 2027 aus. Gerätehersteller, die eine digitale Kommunikationsschnittstelle integrieren müssen, stehen jetzt vor der herausfordernden Aufgabe, zukünftig cybersichere Geräte zu bauen. Unternehmen müssen schon jetzt in Cybersecurity investieren, um ihre Prozesse sowie das bestehende Portfolio zu analysieren und bis 2027 mit den Anforderungen in Einklang zu bringen. Die größte Herausforderung ist der Zeitdruck in Kombination mit der fehlenden Klarheit über eine detaillierte Umsetzung der Cybersicherheitsanforderungen, die auf europäischer Ebene erst noch durch Arbeitsgruppen definiert werden müssen, Stichwort: Harmonized Standards.

ROBERT MÜHLFELLNER, NEURON: Der CRA bietet nun Rechtssicherheit, was wir schätzen – besonders bei Entwicklungsdienstleistungen in der funktionalen Sicherheit. Klare Vorgaben und Standards bieten eine solide Basis für die Produktentwicklung: Dies erleichtert es, unseren Kunden zu vermitteln, warum bestimmte Aspekte bei Neuentwicklungen berücksichtigt werden müssen und warum zusätzliche Kosten entstehen, was früher schwierig zu argumentieren war. Bei der Umsetzung haben funktionale Sicherheit und Cybersecurity zwei gegensätzliche Herausforderungen: lange Produktstabilität ohne Updates und Rezertifizierung versus schnelle Reaktion mit der Notwendigkeit von Updates im laufenden Betrieb an den ‚Toren' zum Produkt. Usable

Bedrohungs- und Risikoanalysen helfen, den Aufwand zu skalieren.

Robert Mühlfellner,
Neuron

Security bedeutet, dass die Security bereits bei der Produktspezifikation definiert werden sollte, um nicht ständig die High-End-Lösung anzustreben, auch die Benutzerfreundlichkeit darf nicht zu kurz kommen, um die Akzeptanz nicht zu gefährden. Ein frühzeitiger Dialog mit Prüfstellen ist notwendig, um die Systemgrenzen gemeinsam zu bestimmen.

DR.-ING. LUTZ JÄNICKE, PHOENIX CONTACT: Der CRA wird die Herangehensweise an die Gestaltung betroffener Produkte erheblich verändern. Das gilt für die Bereitstellung von Security-Funktionen ebenso wie für die Umsetzung eines sicheren Entwicklungsprozesses. Dies wird sich positiv auf die Security und allgemeine Qualität auswirken. Gleichzeitig steigen der Aufwand

Angestrebt werden sollte eine einfache Bedienung der Security-Funktionen.

Lutz Jänicke,
Phoenix Contact

und die fachlichen Anforderungen an Entwickler und Anwender. Eine einfache Bedienung der Security-Funktionen sollte angestrebt werden. Die ausführliche Security-Dokumentation ist sowohl im Gesetz als auch in einschlägigen Standards wie der EN IEC62443 gefordert. Trotzdem bedingt eine gute Sicherheitskonfiguration Zeit und Kenntnis.

DR. RODRIGO DO CARMO, SECUNET: Der CRA legt erstmals verbindliche Cybersicherheitsanforderungen für Produkte mit digitalen Elementen fest. Insbesondere für vernetzte Automatisierungssysteme bedeutet dies eine stärkere Verpflichtung zur Sicherstellung der Produkt- und Systemresilienz über den gesamten Lebenszyklus hinweg. Gleichzeitig ergeben sich auch Chancen für die Anbieter. Einheitliche Anforderungen schaffen eine verlässliche Grundlage für die Integration von Sicherheitsmaßnahmen in der Produktentwicklung und ermöglichen es, sich frühzeitig als Anbieter sicherer Lösungen zu positionieren. Insbesondere Unternehmen, die Sicherheitszertifizierungen nach den neuen Vorgaben umsetzen (wie etwa nach IEC62443), können sich im Markt differenzieren und regulatorische Anforderungen als Qualitätsmerkmal nutzen. Die Umsetzung des CRA bringt jedoch auch erhebliche Herausforderungen mit sich. Er erfordert ein durchgängiges Sicherheitskonzept über den gesamten Produktlebenszyklus hinweg, einschließlich sicherer Softwareentwicklung, Schwachstellenmanagement und langfristiger Update-Strategien. Hinzu kommt der Aufwand für Zertifizierungen und Dokumentationspflichten.

STEFAN BAMBERG, WIBU-SYSTEMS: Um Cyberangriffe abzuwehren, wird ein rechtlicher Rahmen zur Sicherstellung der Cybersicherheit benötigt. Beim CRA geht es um die Sicherheit digitaler Produkte und Dienstleistungen. Inzwischen stecken in den meisten Lösungen der Automatisierungsbranche digitale Komponenten, sodass mehr Unternehmen von der Umsetzung des CRA betroffen sind, als es auf den ersten Blick aussieht. Vorteilhaft für CRA-konforme Lösungen ist ein erhöhtes Verbrauchervertrauen. Zu den Herausforderungen zählen die Updatepflicht, das heißt die Unternehmen müssen rechtzeitig Sicherheitsupdates bereitstellen, und die Notwendigkeit, dass die ausgelieferten Produkte lückenlos und dauerhaft vor Cyberangriffen entlang der Lieferkette geschützt sind. Meiner Meinung nach muss Usable Security gegeben sein, damit die Entwickler einfach und problemlos geeignete Abwehrmaßnahmen in ihre Lösungen einbauen können.

Welche spezifischen Anforderungen des CRA sind für die Fertigungs- und Prozessindustrie relevant und wie lassen sie sich in Produkten und Prozessen effektiv umsetzen? Welche Anpassungen sind bei der Entwicklung, Implementierung und Wartung von Automatisierungssystemen notwendig?

SIMON GÖGGEL, ADS-TEC: Für den Maschinen- und Anlagenbau sind insbesondere die Anforderungen an Identitäts- und Authentifikationskontrollen relevant. Der CRA fordert, dass Produkte mit digitalen Elementen Sicherheitsmaßnahmen beinhalten, jedoch nur dort, wo sie sinnvoll sind. Standards wie IEC62443-4-2 schreiben klare Zugriffskontrollen vor. Ein weiterer Punkt ist die Netzwerksegmentierung. Produktionsnetzwerke müssen so gestaltet werden, dass kritische Systeme isoliert und nur über gesicherte Verbindungen wie VPNs oder Firewalls erreichbar sind. Besonders in der Prozessindustrie ist dies essenziell, um unautorisierten Zugriff auf Steuerungssysteme zu verhindern. Sicherheitsmaßnahmen müssen in der Produktentwicklung berücksichtigt werden. Unternehmen müssen langfristig Sicherheitsupdates garantieren, regelmäßige Software-Patches in den Wartungsprozess integrieren und Lieferketten absichern, damit Zulieferer die Sicherheitsanforderungen erfüllen. Zu den erforderlichen Anpassungen gehören: sichere Software- und Hardwareentwicklung mit Security by Design, Pflicht zur Risiko-

Wer frühzeitig in Cybersecurity investiert, wird langfristig am Markt bestehen.

Simon Göggel,
ADS-Tec

analyse für vernetzte Komponenten, regelmäßige Sicherheitsupdates und Patches, Dokumentation und Auditierung gemäß IEC62443.

FRANK BEHNKE, HILSCHER: Der CRA bringt tiefgreifende Anpassungen in der Produktentwicklung und im Betrieb mit sich. Besonders kritisch ist die Meldepflicht für Sicherheitsvorfälle innerhalb von 24 Stunden, was ein effektives Incident-Management und Security-Monitoring voraussetzt. Ansonsten drohen empfindliche Strafen. Um die Anforderungen zu erfüllen, müssen Unternehmen ihre Entwicklungsprozesse anpassen, indem sie Security-by-Design und Security-by-Default von Anfang an implementieren. Das bedeutet: Risikobewertungen und Sicherheitsaudits bereits in der Entwicklungsphase; nachhaltige Update- und Patch-Strategien, um Produkte über ihren gesamten Lebenszyklus sicher zu halten; Zertifizierungskonformität, da signifikante Änderungen an bestehenden Produkten eine Neuzertifizierung erfordern. In der Praxis braucht es zentralisierte Patch-Management-Systeme, robuste Zugriffs- und Authentifizierungslösungen und klar definierte Prozesse für regelmäßige Sicherheitsüberprüfungen. Gerade für komplexe Automatisierungssysteme ist es entscheidend, Cybersicherheit so zu integrieren, dass sie den Betrieb nicht beeinträchtigt und gleichzeitig die Anforderungen des CRA zuverlässig erfüllt.

THILO DÖRING, HMS: Im Rahmen des CRA wird Cybersecurity integraler Bestandteil der Geräteentwicklung. Das beginnt mit einer Risikoanalyse und

Cybersecurity wird integraler Bestandteil der Geräteentwicklung.

Thilo Döring,
HMS Industrial

umfasst die Spezifikation, die Dokumentation für den fachgerechten Einsatz im Feld sowie die Produktpflege. Letztere muss gewährleisten, dass über den gesamten Lebenszyklus hinweg bekannte Sicherheitslücken in Geräten geschlossen und auch zukünftige Schwachstellen behoben werden. All das wird die Unternehmensprozesse, insbesondere im Bereich Produktentwicklung und Produktmanagement, stark verändern. Diese Prozesse sind heute nur in wenigen Unternehmen schon vorhanden. Die IEC62443 beschreibt in Teil 4-1 den Rahmen, innerhalb dessen Komponentenhersteller bzw. Automatisierungsgerätehersteller ihre Prozesse entsprechend strukturieren sollten. Teil 4-2 des Standards legt die Anforderungen für die Komponenten selbst fest. Damit dient er als Leitfaden, um in Unternehmen mittel- und langfristig eine cybersichere Herangehensweise zu etablieren. Eine Zertifizierung stellt den Nachweis für entsprechende Maßnahmen für mehr Cybersicherheit dar.

ROBERT MÜHLFELLNER, NEURON: Unternehmen müssen einen zusätzlichen Prozess neben dem bestehenden Qualtätsmanagement einführen, um den gesetzlichen Anforderungen für Produkt- und Bedrohungsbeobachtungen gerecht zu werden. Besonders die schnellen Reaktionszeiten bei Sicherheitslücken stellen eine große Herausforderung dar. In Bereichen, in denen Software-Updates bisher adhoc durchgeführt wurden, sind nun klare Cybersecurity-Maßnahmen erforderlich. Auch die IT-Infrastruktur muss angepasst

werden, um Risiken zu minimieren. Für die Entwicklung von funktionalen Sicherheitsprodukten sind klare Strukturen zur Bewertung und Umsetzung von Cybersecurity notwendig, besonders im Kontext der EN62443-Normenreihe. Bedrohungs- und Risikoanalysen helfen, den Aufwand zu skalieren. Eine Schulung durch geeignete Stellen wie TÜV ist erforderlich, um den richtigen Sprachgebrauch und Vorgehensweisen zu verstehen. Die Integration von Cybersecurity in das QM umfasst Maßnahmen über den gesamten Produktlebenszyklus. Während es bei der Entwicklung und Implementierung viele Ähnlichkeiten zur funktionalen Sicherheit gib, erfordert nun die Wartung zusätzlich laufende Beobachtung.

DR.-ING. LUTZ JÄNICKE, PHOENIX CONTACT: Der Ansatz des CRA ist produktgruppenübergreifend und umfasst Verbraucherprodukte ebenso wie Investitionsgüter. Eine genauere Analyse zeigt, dass die Anforderungen des CRA gut von der bestehenden Kombination aus EN IEC62443-4-2 (sichere Komponenten) unter Anwendung der EN IEC62443-4-1 (sicherer Entwicklungsprozess) erfüllt werden. Insofern sind die Rahmenbedingungen im Automatisierungsumfeld bereits bekannt und inhaltlich passend. Es ist somit auch nachvollziehbar, wie Automatisierungssysteme zukünftig entwickelt,

Nötig wird ein durchgängiges Sicherheitskonzept über den gesamten Produktlebenszyklus hinweg.

Dr. Rodrigo do Carmo,
Secunet

Es sind mehr Unternehmen von der Umsetzung des CRA betroffen, als es auf den ersten Blick aussieht.

Stefan Bamberg,
Wibu-Systems

implementiert und gewartet werden müssen. Eine europäische Überarbeitung der genannten Normen sowie der EN IEC62443-3-3 (sichere Systeme) zur vollständigen Abdeckung der Anforderungen des CRA mit dem Ziel eines harmonisierten Standards hat bereits begonnen.

DR. RODRIGO DO CARMO, SECUNET: Die Umsetzung des CRA erfordert eine enge Verzahnung von Entwicklungs-, Produktions- und Wartungsprozessen. Unternehmen sollten frühzeitig sichere Softwareentwicklungsprozesse etablieren, um bereits in der Designphase potenzielle Sicherheitsrisiken zu minimieren. Dazu gehören Maßnahmen wie sichere Programmierpraktiken, Bedrohungsanalysen und Sicherheitsprüfungen in jeder Entwicklungsstufe. Gleichzeitig ist ein effektives Schwachstellenmanagement über den gesamten Produktlebenszyklus hinweg erforderlich. Es ist entscheidend, Update-Mechanismen so zu gestalten, dass sie den laufenden Betrieb nicht beeinträchtigen. Die Anforderungen des CRA machen zudem umfassende Anpassungen in der Entwicklung, Implementierung und Wartung von Automatisierungssystemen notwendig. Die Implementierung sicherer Fernzugriffslösungen, segmentierter Netzwerke und klar definierter Zugriffsrechte wird für viele Unternehmen eine zentrale Herausforderung sein. Gleichzeitig müssen bestehende Prozesse angepasst werden, um Compliance mit den neuen regulatorischen Vorgaben zu gewährleisten.

STEFAN BAMBERG, WIBU-SYSTEMS: Industrielle Steuerungen sind oft ein Ziel von Cyberangriffen und müssen deswegen akribisch geschützt werden. Es ist deswegen wichtig, Security-Maßnahmen gleich im Entwicklungsprozess als Security by Design zu etablieren, um deutlich teurere Korrekturmaßnahmen in einem späteren Designprozess unbedingt zu vermeiden. Um die CRA Compliance kontinuierlich zu gewährleisten, ist ein wohlorganisiertes Assetmanagement erforderlich. Es ist wichtig, jederzeit in einer Anlage zu wissen, welche Komponenten in welcher Version verbaut sind, um einen automatisierten Updateprozess, auch in abgeschotteten Teilen eines Werkes, etablieren zu können. ■

Simon Göggel
Leiter Produktmanagement
ADS-Tec Industrial IT

Frank Behnke
Head of Information Systems
Hilscher Gesellschaft für Systemautomation

Thilo Döring
Geschäftsführer
HMS Industrial Networks

Robert Mühlfellner
CTO
Neuron Automation

Dr.-Ing. Lutz Jänicke
Corporate Product & Solution Security Officer
Phoenix Contact

Dr. Rodrigo do Carmo
Head of Manufacturing and Information Security
Secunet Security Networks

Stefan Bamberg
Director Sales & Key Account Management
Wibu-Systems