EU setzt Deadline für Cyber-Resilienz

Erhöhter Handlungsdruck für die Industrie

Dialog über digitale Produktionsprozesse und Cybersicherheit in der industriellen Automatisierung

Mit dem EU Cyber Resilience Act (CRA) verschärft die Europäische Union die Sicherheitsanforderungen deutlich. Ab Herbst 2026 greifen erste verbindliche Pflichten; ab 2027 dürfen vernetzte Geräte, Maschinen und Anlagen nur noch betrieben oder in Verkehr gebracht werden, wenn sie den CRA-Vorgaben entsprechen.

Die Zeit drängt – und das Risiko ist real. Wer die Anforderungen ignoriert, muss mit drastischen Konsequenzen rechnen: bis zu 15 Millionen Euro oder 2,5 % des weltweiten Jahresumsatzes. Auch eine persönliche Haftung von Geschäftsführern ist vorgesehen.

Der „IoT & OT Cybersecurity Report 2025" des Sicherheitsunternehmens Onekey zeigt: Viele Unternehmen haben erste Maßnahmen gestartet, doch vollständige CRA-Compliance ist noch weit entfernt. Für den Report wurden 300 deutsche Industrieunternehmen zu OT- und IoT-Sicherheit befragt.

Autor:
Jan Wendenburg
CEO
ONEKEY
https://onekey.com/

Countdown zur CRA-Compliance

Nur 32 Prozent der Unternehmen sind mit den CRA-Anforderungen umfassend vertraut, 36 Prozent haben sich zumindest damit befasst, 27 Prozent noch gar nicht. Erst 14 Prozent haben umfangreiche Maßnahmen eingeleitet, 38 Prozent erste Schritte, während ebenso viele noch gar nichts getan haben.

Umfassende Pflichten

Hersteller müssen Produkte von Beginn an sicher konzipieren (Security by Design/Default) und über den gesamten Lebenszyklus absichern. Dies beinhaltet: Schutz vor unbefugtem Zugriff, Wahrung von Datenintegrität und -verfügbarkeit. Aktiv ausgenutzte Schwachstellen und schwerwiegende Vorfälle sind binnen 24 Stunden an ENISA und das zuständige nationale CSIRT zu melden. Pflicht sind zudem regelmäßige Sicherheitsupdates, eine vollständige Dokumentation inklusive Software Bills of Materials (SBOMs) – und die Konformität ist zu dokumentieren und nachzuweisen.

Zentrale Herausforderungen

Im Rahmen der Umfrage wollte Onekey wissen, mit welchen Herausforderungen die Unternehmen in Bezug auf den CRA in der Praxis zu kämpfen haben. 37 Prozent der Unternehmen sehen die 24h-Meldepflicht als größte Hürde, 35 Prozent „Security by Design/Default", 29 Prozent die SBOM-Erstellung. Die Bandbreite betroffener Produkte reicht von Smart-Home-Geräten bis zu Industrierobotern und Produktionsanlagen.

Umdenken gefordert

Cybersicherheit zielte in vielen Segmenten bislang vor allem auf den Schutz der Unternehmens-IT ab, weniger auf die Produkte selbst. Der CRA verlangt nun den Perspektivwechsel: Sicherheit muss von Beginn an ins Produkt. Ab 2027 dürfen nicht konforme vernetzte Geräte, Maschinen und Anlagen in der EU weder verkauft noch betrieben werden. Bei Entwicklungszyklen von zwei bis drei Jahren bleibt kaum Zeit – jetzt ist entschlossenes Handeln gefragt.

CRA-Konformität bedeutet dabei nicht nur regulatorische Pflichterfüllung, sondern auch wirksamen Schutz der Kunden vor wachsender Cyberkriminalität. Allein 2024 verursachten Cyberangriffe in Deutschland Schäden von rund 178,6 Milliarden Euro.

Schlüsselfaktor SBOM

Eine aktuelle SBOM ist zentral für Sicherheit und Compliance. Doch nur 12 % der Unternehmen haben vollständige Transparenz; 44 % befassen sich damit, aber lediglich 12 % haben eine SBOM für alle Produkte – ein Viertel hat noch keine. Die Umsetzung ist komplex: Viele Systeme basieren auf veralteten oder proprietären Komponenten, dazu kommen unvollständige Lieferketten. Hinzu kommt, dass eine SBOM keine einmalige Aufgabe ist, sondern dauerhaft gepflegt werden muss. Allein 2024 wurden mehr als 40.000 neue Schwachstellen gemeldet – Hersteller müssen kontinuierlich prüfen, ob ihre Produkte betroffen sind.

Nachholbedarf bei technischen Standards

Bei der Umsetzung der technischen Anforderungen des CRA zeigt sich in der Industrie Nachholbedarf. Nur 27 Prozent der befragten Unternehmen berücksichtigen die Norm IEC 62443-4-2, obwohl sie eine zentrale Grundlage für die CRA-Compliance darstellt.

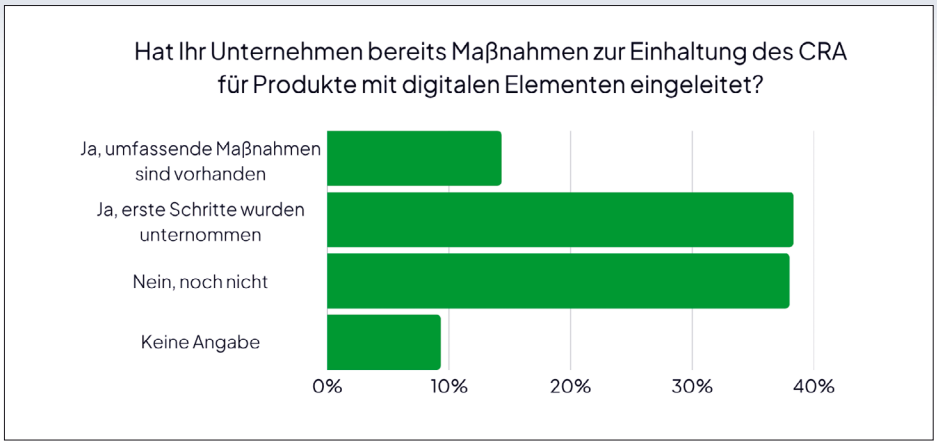
Die Norm legt Sicherheitsanforderungen für Komponenten industrieller Automatisierungs- und Steuerungssysteme (IACS) fest. Sie umfasst sieben Kernpunkte:

- Identifikation & Authentifizierung,
- Zugriffskontrolle,
- Systemintegrität,
- Datenvertraulichkeit,
- eingeschränkter Datenfluss,
- Ereignisreaktion in Echtzeit
- sowie Ressourcenverfügbarkeit.

Ziel ist, die Komponenten so abzusichern, dass sie gängigen Cyberangriffen eigenständig standhalten.

ETSI EN 303 645 findet wenig Beachtung

Ein zweiter für die CRA-Compliance wesentlicher Standard – ETSI EN 303 645 – findet bei der Produktentwicklung ebenfalls wenig Beachtung. Nur ein Viertel der befragten Unternehmen



Hat Ihr Unternehmen bereits Maßnahmen zur Einhaltung des CRA für Produkte mit digitalen Elementen eingeleitet? © ONEKEY IoT & OT Cybersecurity Report 2025

berücksichtigen diese Norm, die Cybersicherheitsanforderungen für vernetzte Verbrauchergeräte festlegt, um grundlegenden Schutz vor Cyberangriffen zu gewährleisten.

Die Norm umfasst **13 Kernanforderungen**, darunter sichere Standardkonfigurationen, Schutz personenbezogener Daten, Software-Updates und sichere Kommunikation. Sie dient als harmonisierte Norm, um die Anforderungen des EU CRA für IoT-Geräte zu erfüllen. Hersteller können die CRA-Compliance und die CE-Kennzeichnung für den EU-Markt nur durch Konformität mit der ETSI EN 303 645 nachweisen.

RED-Funknorm: Aufholbedarf

Auch beim Standard RED (EN 18031) besteht in der Industrie Nachholbedarf. Diese Funkanlagenrichtlinie ist für vernetzte Geräte von großer Bedeutung, da immer mehr Maschinen, Sensoren, Aktoren und andere Digitalprodukte per Funk vernetzt werden. Die Richtlinie soll Störungen im Funkverkehr vermeiden. Sie schreibt vor, dass die Produkte der Hersteller den Anforderungen entsprechen müssen, bevor sie auf den Markt gebracht werden. Dennoch findet RED lediglich bei 16 Prozent der befragten Unternehmen im Zusammenhang mit dem CRA Beachtung.

Verantwortlichkeiten breit gestreut

Im Report geht es auch um Verantwortlichkeiten. 46 Prozent der Unternehmen sagen, die IT-Sicherheit sei für die Erfüllung des CRA verantwortlich. 21 Prozent sagen, die Compliance-Abteilung, 18 Prozent die Geschäftsleitung, 16 Prozent die Rechtsabteilung und 15 Prozent die Produktentwicklung. Die große Bandbreite hängt damit zusammen, dass die Verordnung ein breites Spektrum an Themen berührt.

Hersteller vernetzter Produkte müssen Geräte, Maschinen und Anlagen von Beginn an sicher konzipieren (und über den gesamten Lebenszyklus CRA-konform halten – eine zentrale Aufgabe für Engineering und Produktentwicklung). Ausgenutzte Schwachstellen und schwerwiegende Vorfälle sind binnen 24 Stunden an ENISA und das zuständige nationale CSIRT zu melden.

Regelmäßige Sicherheitsupdates

Zudem sind regelmäßige Sicherheitsupdates Pflicht, um bekannte Lücken zu schließen. Erforderlich ist auch eine vollständige Produktdokumentation inkl. SBOM, die Transparenz und Rückverfolgbarkeit aller Komponenten sicherstellt.

Die dazugehörige Dokumentation liegt im Verantwortungsbereich der Compliance-Abteilung. Bei Verstößen drohen hohe Bußgelder. Das Risiko der persönlichen Haftung von Vorstand bzw. Geschäftsführung ist nicht zu übersehen. Insofern ist es verständlich, wenn die oberste Führungsebene sich ebenfalls in die betriebliche Umsetzung des CRA involviert.

Eine Herausforderung für die Industrie besteht darin, der EU-Verordnung in ihrer gesamten Breite gerecht zu werden.

Der Report zeigt: Es gibt viele Positionen zum Thema CRA. In 18 Prozent der Unternehmen ist der Produktmanager zuständig, in 17 Prozent der Compliance-Verantwortliche, in 15 Prozent der Chief Information Security Officer (CISO) und in 11 Prozent ein Cybersecurity-Analyst. Nur 8 Prozent der Firmen sehen den Leiter Softwareentwicklung als zuständig für den CRA an, obwohl die Software-Stückliste wichtig für die Erfüllung der CRA-Verordnung ist.

Über 40 % mit CRA-Organisation

Onekey hat in seiner Industrieumfrage geprüft, wie Unternehmen den abteilungsübergreifenden CRA-Handlungsbedarf organisatorisch abbilden: 28 Prozent haben eine bereichsübergreifende Arbeitsgruppe, 13 Prozent ein dediziertes CRA-Team; 32 Prozent verfügen noch über keine spezielle Struktur. Bei 18 Prozent arbeiten vier bis zehn Personen an der Umsetzung, bei 15 Prozent bis zu drei, bei 8 Prozent mehr als zehn (u. a. Entwicklung, SBOM, Compliance). Insgesamt sind über 40 Prozent mit einer eigenen CRA-Organisation aufgestellt – ein notwendiger Schritt, denn Cybersicherheit dient längst nicht nur der Compliance, sondern dem Schutz vor zunehmend raffinierten Angriffen.

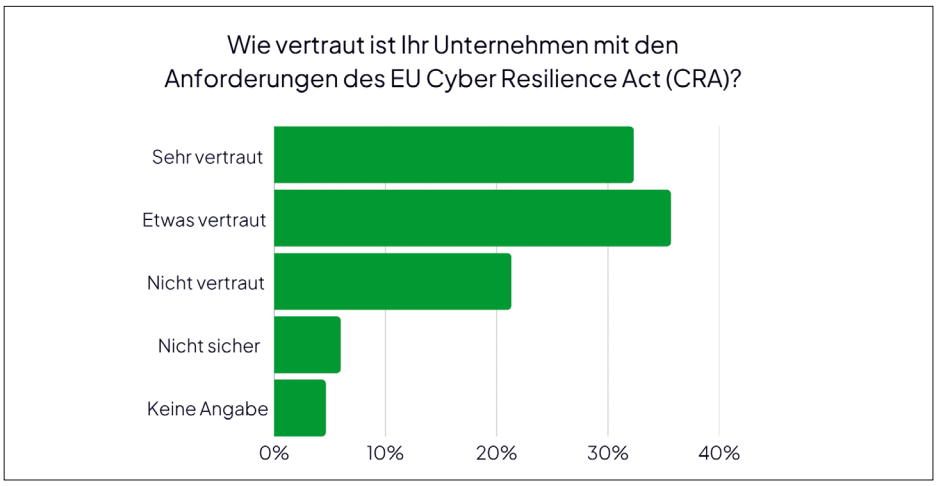
Weiterbildung ist wichtig

Eine weitere Erkenntnis aus dem „IoT & OT Cybersecurity Report“: Die Unternehmen sollten mehr in die Weiterbildung ihrer Beschäftigten in Bezug auf Cybersecurity und insbesondere den CRA investieren. Bislang führt nicht einmal ein Drittel (30 Prozent) der befragten 300 Unternehmen mindestens einmal jährlich eine Weiterbildungsmaßnahme in Sachen CRA für seine Beschäftigten durch. Weitere 28 Prozent halten eine diesbezügliche Schulung alle ein bis zwei Jahre für ausreichend.

Fazit

Die Industrie befindet sich auf gutem Weg, den Anforderungen des Cyber Resilience Act nachzukommen. Aber sie sollte kräftig an Tempo zulegen, um dieses Ziel rechtzeitig zu erreichen.

Denn beim CRA handelt es sich um eine EU-Verordnung, nicht bloß um eine Richtlinie. Das bedeutet, dass diese Cybersicherheitsnorm keine nationale Umsetzung benötigt, sondern entlang der EU-Zeitvorgaben unmittelbar rechtswirksam wird. Es wird also keine Zeitverzögerung durch eine deutsche Umsetzung des CRA geben, wie es beispielsweise bei der Cybersicherheitsnorm NIS2 der Fall ist. „Tempo, tempo, tempo!“ möchte man der Industrie angesichts dieser Situation zurufen. ◄



Wie vertraut ist Ihr Unternehmen mit den Anforderungen des EU Cyber Resilience Act (CRA)? © ONEKEY IoT & OT Cybersecurity Report 2025