ONEKEY.COM

IOT & OT CYBERSECURITY REPORT 2025

Die Zeit drängt: 68% der Unternehmen sind mit dem neuen Cyber Resilience Act noch nicht vertraut

ONEKEY

CYBERSECURITY REPORT

ZUSAMMENFASSUNG

IoT & OT Cybersecurity Report 2025

Lesezeit: ca. 15 min.

Auf dem Weg zur Compliance mit dem EU Cyber Resilience Act (CRA) sollten die Unternehmen jetzt einen „Endspurt“ hinlegen, um die Fristen einhalten zu können. Doch in der Wirtschaft ist davon noch wenig zu spüren. Bei einer Umfrage unter 300 Industrieunternehmen kam heraus, dass nur ein knappes Drittel (32 Prozent) der Unternehmen mit den Anforderungen des EU Cyber Resilience Act umfassend vertraut ist. Dementsprechend zögerlich ist die Umsetzung. Lediglich 14 Prozent der befragten Firmen haben bereits umfangreiche Maßnahmen eingeleitet, um für die Einhaltung der CRA-Vorschriften bei ihren vernetzten Geräten, Maschinen und Anlagen zu sorgen.

„Bislang haben viele Hersteller digitaler Geräte, Maschinen und Anlagen vor allem die Funktionalität ihrer Produkte in den Fokus gestellt und die Angreifbarkeit durch Cyberattacken weniger stark im Auge gehabt. Mit dem Cyber Resilience Act ist es nun zwingend erforderlich, beide Aspekte als gleichwertig einzustufen.“

— Jan Wendenburg, CEO, ONEKEY

ONEKEY wollte im Rahmen der Umfrage wissen, was die größten Herausforderungen sind. Für 37 Prozent der Unternehmen steht demnach die Meldepflicht bei sicherheitskritischen Vorfällen innerhalb von 24 Stunden an erster Stelle. Gleich darauf folgt mit 35 Prozent die Einhaltung der Kriterien „Secure by Design“ und „Secure by Default“. 29 Prozent der Befragten stufen die Erstellung einer Software Bill of Materials als größte Herausforderung ein. Beinahe genauso viele Firmen sehen ein Hauptproblem darin, den Überblick über die Verwaltung von Software-Schwachstellen zu behalten. Lediglich 12 Prozent der Unternehmen haben einen lückenlosen Überblick über die in ihren Geräten, Maschinen und Anlagen verwendeten Programme.

HINTERGRUND ZUM NEUEN EU CYBER RESILIENCE ACT

Erste Verpflichtungen aus dem EU Cyber Resilience Act werden im Herbst 2026 verbindlich, alle weiteren ab 2027. Vernetzte Geräte, Maschinen und Anlagen, die nicht den Anforderungen des CRA entsprechen, dürfen dann in der EU nicht mehr verkauft oder betrieben werden. Beim Cyber Resilience Act handelt es sich um eine EU-Verordnung, keine Richtlinie. Das bedeutet, dass er direkt und unverzüglich in allen EU-Mitgliedstaaten gilt. Eine Verzögerung durch eine nationale Umsetzung, wie es bei NIS2 der Fall ist, wird es beim CRA also nicht geben. Daher ist höchste Eile geboten.

„Vernetzte Geräte, Maschinen und Anlagen, die nicht den Anforderungen des CRA entsprechen, dürfen künftig in der EU nicht mehr verkauft oder betrieben werden. Angesichts von Entwicklungszeiten von zwei bis drei Jahren ist höchste Eile geboten.“

— Jan Wendenburg, CEO, ONEKEY

Bei Verstößen drohen empfindliche Bußgelder von bis zu 15 Millionen Euro oder 2,5 Prozent des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist. Hinzu kommt das Risiko der persönlichen Haftung von Vorstand bzw. Geschäftsführung und/oder den Verantwortlichen. Die aktuelle Umfrage von ONEKEY belegt, dass die Wirtschaft zwar bereits Maßnahmen zur Umsetzung des Cyber Resilience Act ergriffen hat, jedoch weiterhin erheblicher Handlungsbedarf besteht.

DIGITALE TRANSFORMATION VERGRÖSSERT DIE ANGRIFFSFLÄCHE FÜR CYBERBEDROHUNGEN

Internet of Things (IoT) und Operational Technology (OT) stehen im Zentrum der digitalen Transformation industrieller Prozesse. Gleichzeitig wächst die Angriffsfläche für Cyberbedrohungen. ONEKEY hat im Rahmen einer umfassenden Studie den Status quo der IoT- & OT Sicherheit im deutschsprachigen Raum untersucht. Befragt wurden 300 Führungskräfte aus Industrie, IT, OT und Engineering. Der vorliegende Report analysiert die zentralen Erkenntnisse, bewertet Risiken und zeigt Handlungsoptionen auf.

Ein Schwerpunkt der Befragung lag auf dem Cyber Resilience Act, der EU-Verordnung zur Stärkung der Cybersicherheit vernetzter Produkte. Er verpflichtet Hersteller und Inverkehrbringer digitaler Produkte mit Internetanschluss (vernetzte Geräte, Maschinen und Anlagen) zu umfangreichen Sicherheitsmaßnahmen.

PFLICHTEN DER HERSTELLER BZW. INVERKEHRBRINGER

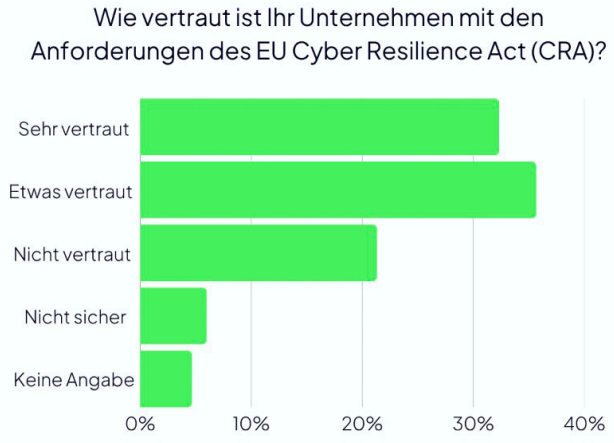
Gemäß Cyber Resilience Act müssen Hersteller ihre Produkte so entwickeln, dass sie von Anfang an sicher sind (Security by Design und Secure by Default) und während ihres gesamten Lebenszyklus den Anforderungen des CRA entsprechen. Dies beinhaltet den Schutz vor unbefugtem Zugriff, den Schutz der Datenintegrität und -vertraulichkeit sowie die Gewährleistung der Verfügbarkeit der Funktionen.

Zudem sind sie verpflichtet, aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle, die die Sicherheit ihrer Produkte beeinträchtigen, innerhalb von 24 Stunden der europäischen Cybersecurity-Behörde ENISA und dem zuständigen nationalen CSIRT (Computer Security Incident Response Team) zu melden.

Darüber hinaus müssen die Anbieter regelmäßig Sicherheitsupdates bereitstellen, um bekannte Schwachstellen zu beheben und die Sicherheit ihrer Produkte zu gewährleisten. Dazu gehört auch eine umfassende Dokumentation der Produkte, einschließlich einer Software-Stückliste (Software Bill of Materials, SBOM), um die Transparenz und Rückverfolgbarkeit von Komponenten zu gewährleisten. Die Konformität mit den CRA-Anforderungen muss dokumentiert und nachgewiesen werden. Angesichts von in der Regel mehrjährigen Entwicklungszeiten hinken viele Unternehmen hinterher.

NUR EIN DRITTEL IST MIT DEM CRA VERTRAUT

Laut Umfrage ist nur ein knappes Drittel (32 Prozent) der Unternehmen mit den Anforderungen des EU Cyber Resilience Act umfassend vertraut. Weitere 36 Prozent haben sich zumindest schon einmal damit befasst. Mehr als ein Viertel (27 Prozent) hat sich dem Thema jedoch noch gar nicht zugewendet.

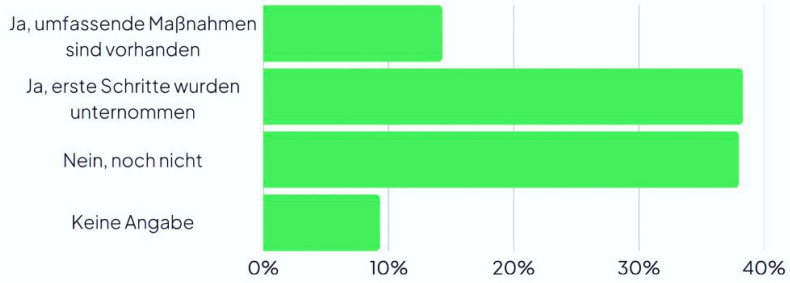


Source: OT und IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

ZÖGERLICHE UMSETZUNG

Dementsprechend zögerlich ist die Umsetzung. Lediglich 14 Prozent (!) der befragten Firmen haben bereits umfangreiche Maßnahmen eingeleitet, um für die Einhaltung der CRA-Vorschriften bei ihren vernetzten Geräten, Maschinen und Anlagen zu sorgen. Immerhin: 38 Prozent sind bereits erste Schritte in Richtung CRA-Compliance gegangen. Allerdings haben ebenso viele Unternehmen bislang noch nichts unternommen, um den neuen EU-Regularien zu genügen.

Hat Ihr Unternehmen bereits Maßnahmen zur Einhaltung des CRA für Produkte mit digitalen Elementen eingeleitet?



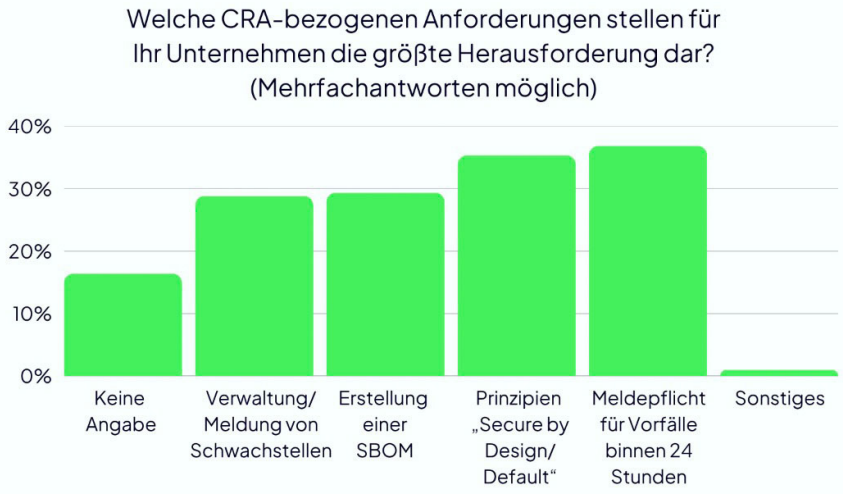
Source: OT und IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

BEDROHUNGSLAGE VERSCHÄRFT SICH WEITER

Diese Zurückhaltung ist nicht nur wegen der strengen gesetzlichen Anforderungen und den drohenden Konsequenzen bei Nichteinhaltung problematisch, sondern auch angesichts einer zunehmenden Bedrohung durch Hacker und den möglichen Schaden. Behörden wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Bundeskriminalamt (BKA) gehen davon aus, dass sich die Sicherheitslage in den nächsten Jahren weiter zuspitzen wird. Bereits 2024 belief sich der Gesamtschaden durch Cybercrime-Vorfälle in Deutschland auf geschätzte 178,6 Milliarden Euro – ein Anstieg von 30,4 Milliarden Euro gegenüber dem Vorjahr.

SBOM BEREITET 29 PROZENT DER FIRMEN SORGEN

Als größte Herausforderung beim Cyber Resilience Act stufen 37 Prozent der von ONEKEY befragten Unternehmen die Meldepflicht binnen 24 Stunden ein. An zweiter Stelle steht die Erfüllung der Prinzipien „Secure by Design“ und „Secure by Default“ (35 Prozent). 29 Prozent bereitet die Erstellung einer Software Bill of Materials (SBOM) und die damit verbundene Pflicht, die Übersicht über alle Software-Komponenten und deren Schwachstellen zu behalten, Sorgen.



Source: OT und IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

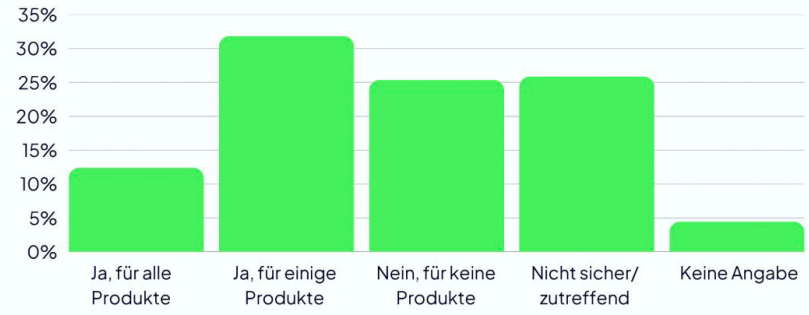
Eine Software Bill of Materials (SBOM) ist eine strukturierte Auflistung aller Software-Komponenten, die in einem digitalen Produkt enthalten sind – inklusive Bibliotheken, Abhängigkeiten und Versionen. Sie fungiert gewissermaßen als „Stückliste“ für Software. Die SBOM ist von zentraler Bedeutung: Sie ermöglicht Transparenz, beschleunigt das Schwachstellenmanagement und ist Voraussetzung für eine schnelle Reaktion bei Sicherheitsvorfällen. Ohne SBOM bleibt unklar, ob eine Sicherheitslücke das eigene Produkt betrifft – mit potenziell gravierenden Folgen für Hersteller, Inverkehrbringer und Kunden. Die Etablierung standardisierter SBOM-Prozesse ist daher ein entscheidender Schritt hin zu resilienter Software-Sicherheit insbesondere in Produktionsumgebungen.

„Der CRA verlangt eine detaillierte Auflistung aller Programme, Bibliotheken und Abhängigkeiten mit genauen Versionsnummern der einzelnen Komponenten, Informationen zu den jeweiligen Lizenzen und einen dokumentierten Überblick inklusive Einschätzung über alle bekannten Schwachstellen und Sicherheitslücken.“ — Jan Wendenburg, CEO, ONEKEY

Die Umfrage hat ergeben, dass 44 Prozent der Unternehmen mit der Erstellung einer SBOM für ihre Produktpalette begonnen haben. Jedoch haben nur 12 Prozent (!) dies für alle Produkte abgeschlossen, während bei 32 Prozent bislang lediglich einzelne Produkte berücksichtigt wurden. Ein Viertel hat noch gar nicht gestartet, ein weiteres Viertel fühlt sich nicht betroffen oder ist unsicher diesbezüglich.

SBOM: VIELE UNTERNEHMEN TAPPEN NOCH IM DUNKELN

Verwendet oder erstellt Ihr Unternehmen derzeit eine Software Bill of Materials (SBOM) für Produkte mit digitalen Elementen, wie es der CRA verlangt?



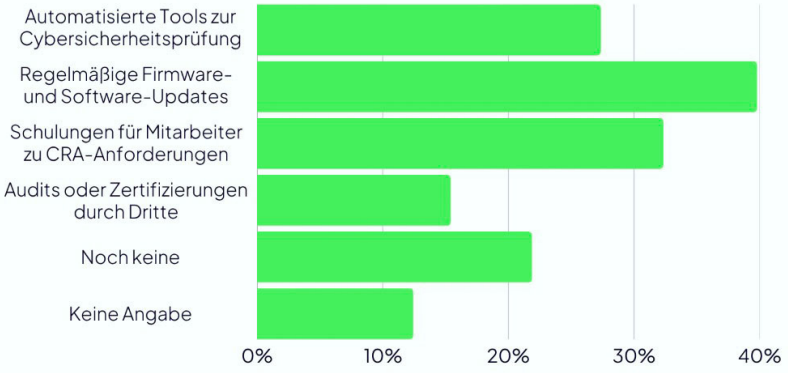
Source: OT und IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

Trotz der eindeutigen Vorgabe des CRA, eine Software Bill of Materials (SBOM) vorzuhalten, hat etwa die Hälfte der Unternehmen in diesem Bereich noch keinen klaren Überblick. Das ist umso bemerkenswerter, als Transparenz über eingesetzte Software-Komponenten und strukturierte Sicherheitsprozesse zu den zentralen Bausteinen moderner Cyberresilienz zählen – bislang jedoch in vielen Betrieben noch nicht ausreichend verankert sind.

RICHTUNG STIMMT, SPEED MUSS ERHÖHT WERDEN

Obgleich noch viele Unzulänglichkeiten und Lücken bestehen, zeigt der Report, dass sich viele Unternehmen auf den Weg in Richtung CRA-Compliance gemacht haben. 40 Prozent führen laut Umfrage regelmäßige Firmware- und Software-Updates durch. 27 Prozent setzen automatisierte Tools zur Cybersicherheitsprüfung ein. 16 Prozent verlassen sich auf Audits und Zertifizierungen von dritter Seite.

Welche Maßnahmen hat Ihr Unternehmen ergriffen, um die Einhaltung des CRA sicherzustellen? (Mehrfachantworten möglich)

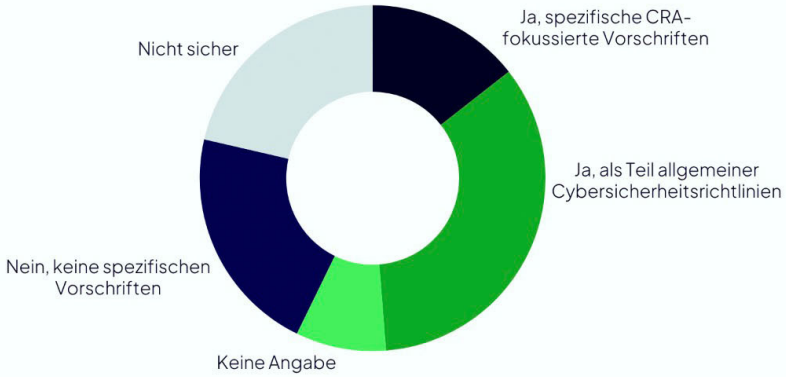


Source: OT und IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

SPEZIFISCHE CRA-COMPLIANCE BISLANG DIE AUSNAHME

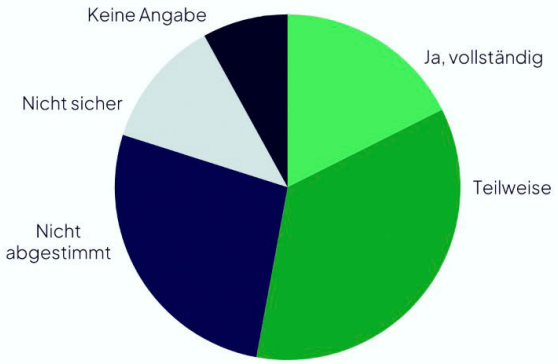
Allerdings verfügen lediglich 15 Prozent der Firmen über CRA-spezifische Compliance-Vorschriften. Aber mehr als ein Drittel (34 Prozent) decken nach eigener Einschätzung die CRA-Vorgaben im Rahmen ihrer allgemeinen Cybersicherheitsrichtlinien ab. 21 Prozent haben den Cyber Resilience Act noch nicht in ihrer Compliance berücksichtigt.

Verfügt Ihr Unternehmen über spezifische Compliance-Vorschriften für CRA-bezogene Cybersicherheitsanforderungen?



Source: OT und IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

Sind die Cybersicherheitsrichtlinien Ihres Unternehmens mit den CRA-Anforderungen für Produkte mit digitalen Elementen abgestimmt?

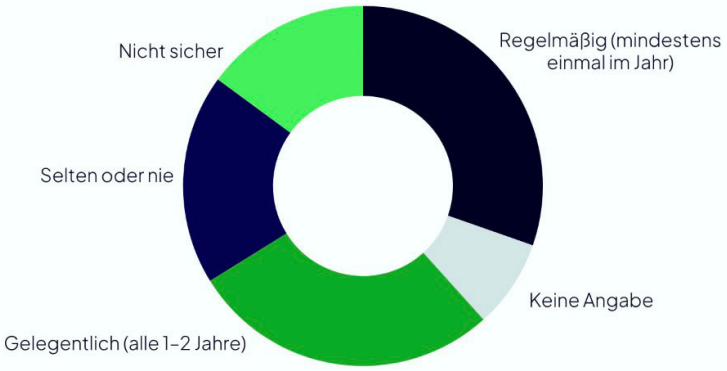


Source: OT und IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

KNAPPES DRITTEL HAT MIT CRA-SCHULUNGEN BEGONNEN

Ein knappes Drittel (32 Prozent) der befragten Unternehmen haben damit begonnen, ihre Belegschaft gezielt mit Schulungen auf die CRA-Anforderungen vorzubereiten. 30 Prozent führen regelmäßig – mindestens einmal im Jahr – entsprechende Weiterbildungsmaßnahmen durch. Weitere 28 Prozent geben an, gelegentlich CRA-Qualifizierungen anzubieten (alle zwei bis drei Jahre). Beinahe ein Fünftel (19 Prozent) verzichtet auf Know-how-Transfer in Sachen Cyber Resilience Act.

Wie oft werden Schulungen oder Weiterbildungen zum CRA für das zuständige Team oder die zuständigen Mitarbeiter durchgeführt?



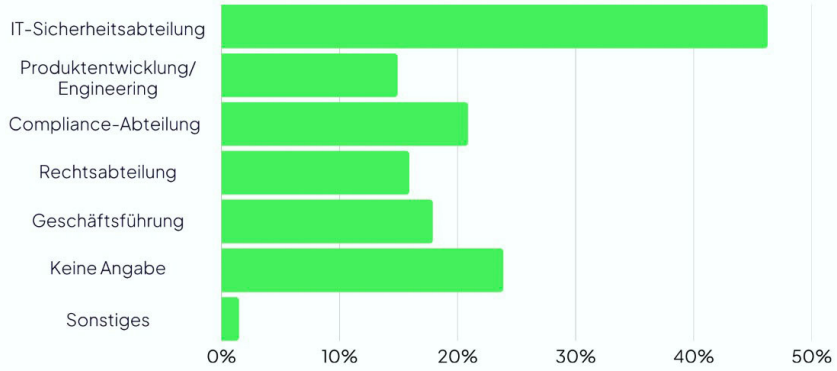
Source: OT und IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

VERANTWORTUNGS-FRAGE WIRD UNTERSCHIEDLICH BEANTWORTET

Die Frage, wer und welche Abteilung für die Erfüllung der CRA-Richtlinie verantwortlich zeichnet, beantworten die Unternehmen sehr unterschiedlich. Bei 46 Prozent der Firmen ist die IT-Sicherheit zuständig, bei 21 Prozent die Compliance, bei 16 Prozent die Rechtsabteilung. Bei 18 Prozent kümmert sich die Geschäftsführung persönlich darum, 15 Prozent haben die Zuständigkeit an die Produktentwicklung abgetreten. Es ist wohl davon auszugehen, dass in vielen Fällen die Verantwortung für die CRA-Compliance über mehrere Abteilungen hinweg verteilt ist.

„Die EU hat mit dem Cyber Resilience Act ein sehr umfangreiches Regelwerk geschaffen, von technischen Normen bis hin zu Meldepflichten. Dementsprechend hoch sind die Herausforderungen für die Industrie, den CRA vollumfänglich umzusetzen.“
— Jan Wendenburg, CEO, ONEKEY

Welche Abteilungen oder Funktionen in Ihrem Unternehmen tragen die Hauptverantwortung für die Einhaltung der CRA-Anforderungen? (Mehrfachantworten möglich)

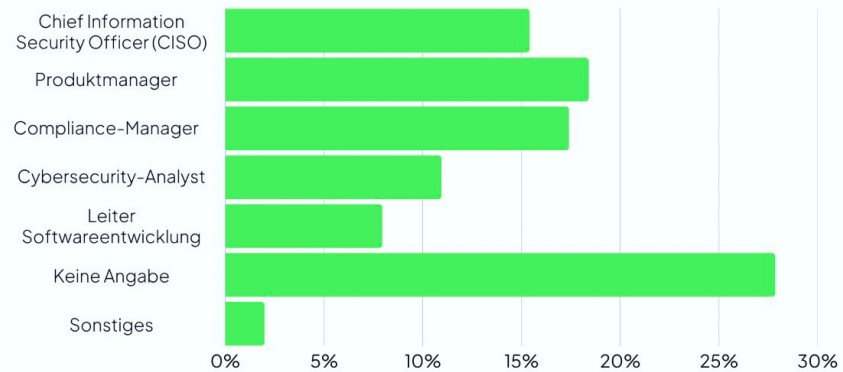


Source: OT und IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

DIFFUSE LAGE BEI DEN ZUSTÄNDIGEN POSITIONEN

Dementsprechend diffus stellt sich die Lage bei den verantwortlichen Positionen dar. 18 Prozent der Firmen weisen die Zuständigkeit für die CRA-Compliance dem Produktmanager zu, 17 Prozent dem Compliance-Manager, 15 Prozent dem Chief Information Security Officer (CISO), 11 Prozent dem Cyberrsecurity-Analysten und 8 Prozent dem Leiter der Softwareentwicklung. Auch hier ist sicherlich in vielen Fällen von überlappenden Verantwortungen auszugehen.

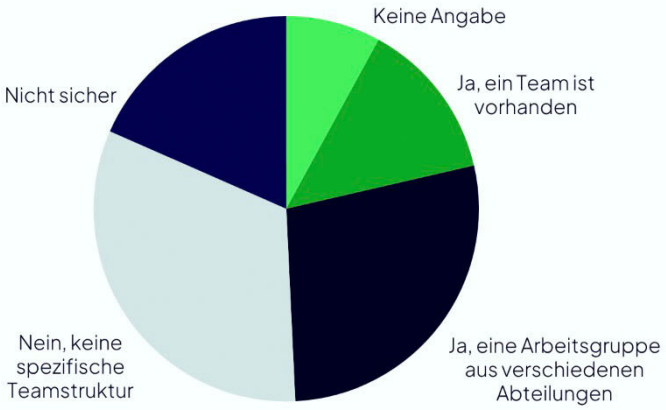
Welche Rollen oder Funktionen sind in Ihrem Unternehmen direkt für die Umsetzung der CRA-Compliance zuständig? (Mehrfachantworten möglich)



Source: OT und IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

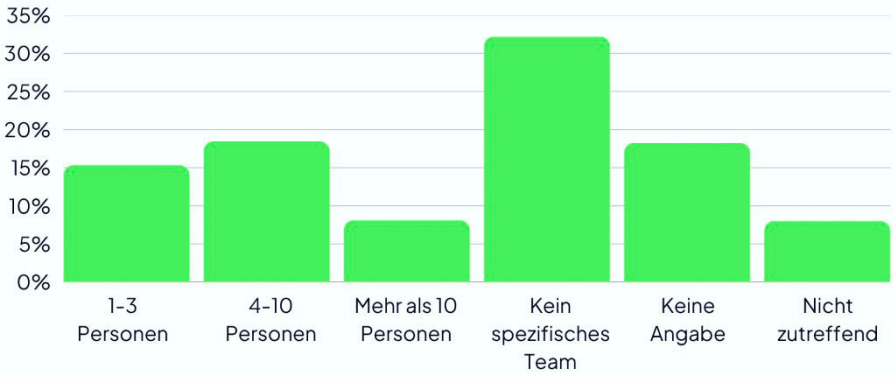
Tatsächlich haben 28 Prozent der befragten Unternehmen eine Arbeitsgruppe aus verschiedenen Abteilungen zusammengestellt, um die Firma „CRA-fit“ zu machen. In 14 Prozent der Firmen ist ein eigenes Team im Einsatz, das sich dezidiert der Erfüllung der CRA-Normen widmet. Die häufigste Teamstärke liegt bei vier bis zehn Personen (in 18 Prozent aller Fälle). Ein knappes Drittel (32 Prozent) haben keine Arbeitsgruppe für den Cyber Resilience Act eingerichtet.

Verfügt Ihr Unternehmen über ein dediziertes Team oder eine Arbeitsgruppe, die sich mit der Umsetzung des CRA befasst?



Source: OT und IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

Wie groß ist das Team oder die Arbeitsgruppe, die sich in Ihrem Unternehmen mit der CRA-Compliance befasst?



Source: OT und IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

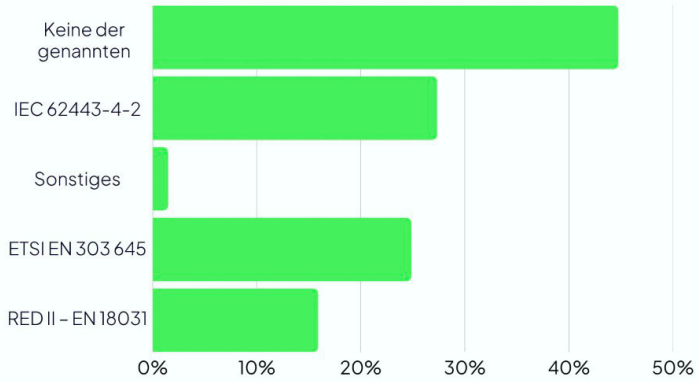
HANDLUNGS-EMPFEHLUNGEN

Auf Basis der Studienergebnisse ergeben sich für Unternehmen folgende zentrale Empfehlungen:

1. Secure by Design / Secury by Default als Basis

Konsequente Ausrichtung aller Produktentwicklungen bei vernetzten Geräten, Maschinen und Anlagen an den Grundsätzen der Cybersicherheit in allen Design-, Entwicklungs-, Produktions- und Wartungsphasen.

Welche für den CRA relevanten Standards berücksichtigt Ihr Unternehmen in der Produktentwicklung? (Mehrfachantworten möglich)



Source: OT und IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

2. Transparenz schaffen

Nur die Einführung lückenloser SBOMs, regelmäßige Schwachstellen-Scans und klare Produktdokumentationen schaffen die vom CRA zwingend vorgeschriebene Transparenz.

3. Automatisierte Sicherheits- und Compliance-Prüfungen

Um den CRA-Pflichten nachzukommen – insbesondere der Meldepflicht und der Gewährleistung der Cybersicherheit über den gesamten Produktlebenszyklus hinweg – ist eine regelmäßige, idealerweise automatisierte, Überprüfung der bekannten und neu gemeldeten Schwachstellen unerlässlich. Dazu gehört auch die Beurteilung zur Relevanz und deren Dokumentation.

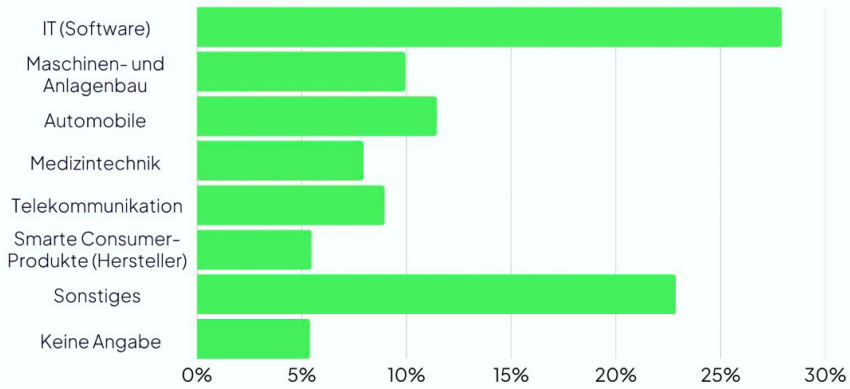
4. Verantwortung klären

Es empfiehlt sich die Benennung eines Produkt Sicherheitsbeauftragten mit OT-/IoT-Kompetenz. Ebenso sinnvoll sind abgestimmte Rollen zwischen IT, OT und Entwicklung in Bezug auf den CRA.

5. Kompetenz aufbauen – auch mit externen Partnern

Schulungen, Weiterbildung und Partnerschaften mit spezialisierten Dienstleistern sind essenziell – auch zur Kompensation des Fachkräftemangels. Ohne externe Unterstützung und Einsatz automatisierter Lösungen – insbesondere zur Erstellung und permanenten Pflege lückenloser Software Bills of Materials und der Überwachung der bekannten und neuen Schwachstellen in allen digitalen Produkten – wird die CRA-Compliance kaum zu erreichen sein.

In welchem Sektor ist Ihr Unternehmen tätig?



Source: OT und IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

TIME TO ACT!

Rund zwei Drittel der Unternehmen sind mit dem Cyber Resilience Act vertraut, die Hälfte davon allerdings nur teilweise. **Höchste Zeit für alle Firmen, sich auf den CRA einzustellen!**

Gut die Hälfte aller befragten Firmen haben bereits erste Maßnahmen eingeleitet, um dem CRA zu genügen; aber nur 15 Prozent sind dabei schon weit fortgeschritten. **Tempo bei der Umsetzung beschleunigen!**

Das Sicherheitprinzip „Secure by Design / Default“ stellt die größte Herausforderung dar, gefolgt von der Erstellung einer SBOM. Ein knappes Drittel besitzt zumindest für einige Produkte eine SBOM; aber nicht einmal 15 Prozent haben eine SBOM für ihre gesamte Produktpalette. **Dringend handeln: Engineering auf „Secure by Design / Default“ einstellen und schnellstmöglich eine SBOM für alle vernetzten Produkte generieren!**

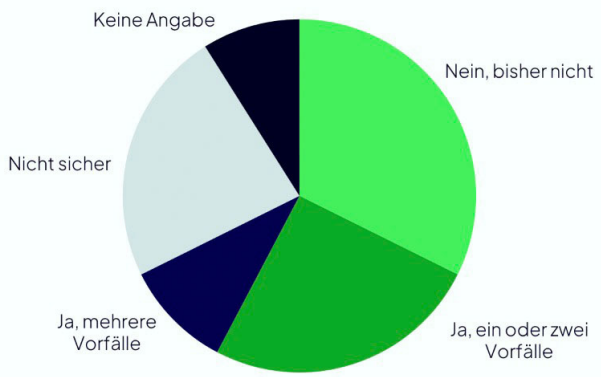
In knapp der Hälfte der Unternehmen liegen CRA-bezogene Compliance-Vorschriften vor, überwiegend allerdings nur allgemein gefasst. **CRA-Compliance zur Top-Priorität erklären!**

40 Prozent führen regelmäßig Firmware- und Software-Updates durch. 27 Prozent setzen automatische Tools zur Überprüfung der Cybersicherheit ein. **Auf automatisierte Lösungen umstellen – andernfalls ist CRA-Compliance nicht zu erreichen!**

Ein Drittel schulen ihre Belegschaft in Bezug auf CRA-Compliance. **Mehr Schulung ist angesagt!**

Mehr als ein Drittel der Unternehmen hat Sicherheitsvorfälle aufgrund der Nichteinhaltung von CRA-Vorschriften erlebt. Die Verantwortung für die Einhaltung der CRA-Anforderungen liegt in fast der Hälfte der Firmen bei der IT-Abteilung. **CRA-Compliance betrifft nicht nur die IT – alle betroffenen Abteilungen einbeziehen!**

Hat Ihr Unternehmen bereits Cybersicherheitsvorfälle im Zusammenhang mit der Nichteinhaltung von CRA-Anforderungen erlebt?



Source: OT und IoT Cybersecurity Report 2025/26, powered by ONEKEY | n = 300

ONEKEY
onekey.com
+49 211 1587 41 04
info@onekey.com

SecurITy made in Germany

20250900IDE