

# IOT & OT CYBERSECURITY REPORT 2026

Endspurt zur CRA-Compliance:  
Industrie auf dem richtigen Weg, aber  
Umsetzung muss schneller werden

ONEKEY

CYBERSECURITY REPORT

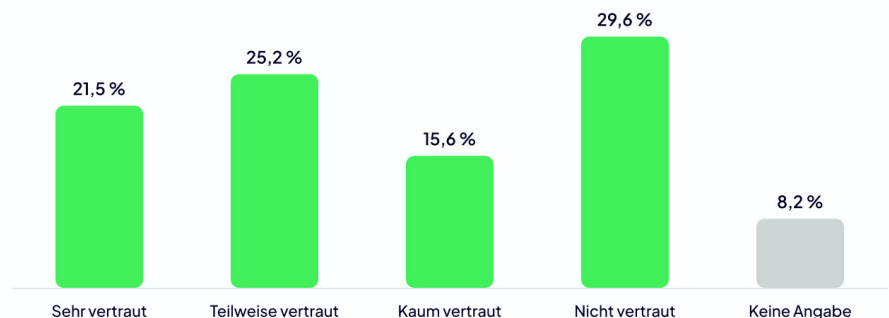
# ZUSAMMENFASSUNG

## IoT & OT Cybersecurity Report 2026

**Lesezeit:** ca. 15 min.

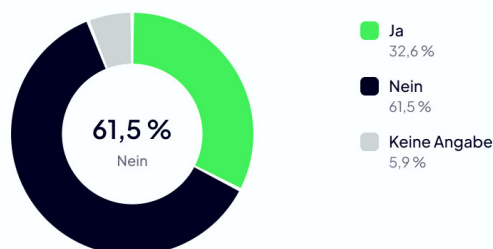
Die deutsche Industrie befindet sich bei der Umsetzung des Cyber Resilience Act (CRA) auf dem richtigen Weg. Angesichts der nahenden Fristen ist dennoch Eile geboten; der Nachholbedarf ist groß. Das zeigt der „IoT & OT Cybersecurity Report 2026“ von ONEKEY, für den 200 deutsche Industrieunternehmen zu ihrer Strategie und Umsetzung rund um die neue EU-Cybersicherheitsverordnung befragt wurden. 46 Prozent der Unternehmen kennen sich mit dem CRA aus, 21 Prozent sogar sehr gut. Gleichzeitig räumen 60 Prozent ein, dass ihnen die weiteren Phasen und Fristen der Regulierung nicht bekannt sind.

**Wie vertraut ist Ihr Unternehmen mit den Anforderungen des EU Cyber Resilience Act (CRA)?**



Quelle: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

**Wissen Sie, wann die weiteren CRA-Phasen vollständig in Kraft treten?**



Quelle: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

**„Die deutsche Industrie hat den Cyber Resilience Act inzwischen auf dem Radar. Jetzt kommt es darauf an, aus Awareness konsequente Umsetzung zu machen. Wer die verbleibende Zeit bis Ende 2027 nicht nutzt, riskiert später erhebliche Verzögerungen bei Entwicklung und Markteinführung.“**

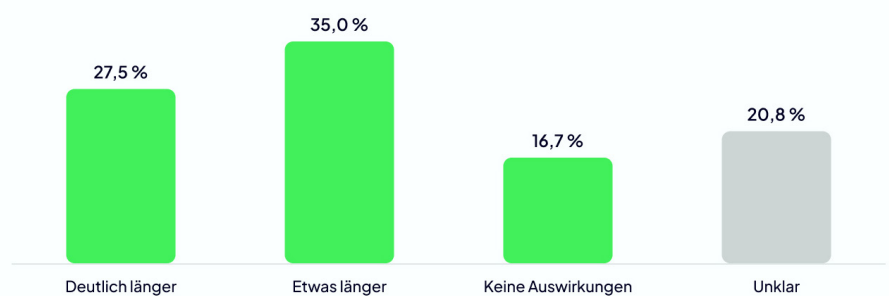
**— Jan Wendenburg, CEO, ONEKEY**

Die Defizite zeigen sich vor allem in der praktischen Umsetzung. Zwar haben viele Unternehmen erste Maßnahmen eingeleitet, doch in zentralen Bereichen wie Risikomanagement, Dokumentation, Sicherheitsupdates und technischen Nachweisen besteht weiterhin erheblicher Nachholbedarf. Besonders herausfordernd sind die ab dem 11. September 2026 geltende Meldepflicht für Sicherheitsvorfälle binnen 24 Stunden, das Vulnerability Management, Software-Stücklisten sowie „Security by Design / Security by Default“.

Hinzu kommt die Lieferkette. Hersteller müssen nicht nur ihre eigenen Entwicklungen absichern, sondern auch Risiken aus zugelieferter Software, Firmware und weiteren Komponenten beherrschen. Nur rund 18 Prozent der Zulieferer haben sich nach Einschätzung der befragten Unternehmen konsequent auf die CRA-Anforderungen eingestellt und liefern die notwendigen Informationen.

Gleichzeitig rechnen weit über 60 Prozent der Unternehmen mit einem höheren Zeitaufwand für die Entwicklung neuer oder aktualisierter Produkte. Die CRA-Compliance wird damit nicht nur zur regulatorischen Aufgabe, sondern greift tief in Produktentwicklung, Beschaffung, Lieferantenmanagement und interne Verantwortlichkeiten ein.

**Welche Auswirkungen erwarten Sie auf die Markteinführung neuer Produkte?**



Quelle: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

**„Mit dem Cyber Resilience Act endet die Vorstellung, dass Hersteller die Verantwortung für unsichere Software-Komponenten einfach an Zulieferer weitergeben können. Wer ein Produkt unter eigenem Namen auf den europäischen Markt bringt, trägt die Verantwortung für die Cybersicherheit des gesamten Produkts.“**

**— Jan Wendenburg, CEO, ONEKEY**

# HINTERGRUND ZUM NEUEN EU CYBER RESILIENCE ACT

Der Cyber Resilience Act betrifft Geräte, Maschinen und Anlagen mit digitalen Internet-Komponenten ebenso wie Software und weitere vernetzte Produkte. Dazu zählen unter anderem vernetzte Maschinen und Steuerungen, Router, Firewalls und Netzwerkgeräte, IoT- und Smart-Home-Geräte, Betriebssysteme, Apps, industrielle Steuerungssoftware und Cloud-Funktionen, sofern sie für die Funktion eines Produkts notwendig sind.

Vollständig greift die CRA-Regulierung am 11. Dezember 2027. Ab diesem Stichtag dürfen keine neuen Produkte mit Internetverbindung in den 27 Ländern der Europäischen Union verkauft werden, wenn sie die Anforderungen des Cyber Resilience Act nicht erfüllen. Eine wichtige Pflicht gilt jedoch bereits seit dem 11. September 2026: Inverkehrbringer digitaler Produkte müssen aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle melden. Von Ausnahmen abgesehen betrifft dies auch Produkte, die bereits auf dem Markt sind.

Für Hersteller, Händler und Importeure bedeutet der CRA, dass sie ihre Produkte umfassend vor Hackerangriffen schützen und die Sicherheit nachweisen und dokumentieren müssen. Bei Verstößen gegen grundlegende Cybersicherheitsanforderungen oder zentrale Herstellerpflichten drohen bis zu 15 Millionen Euro oder 2,5 Prozent des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist.

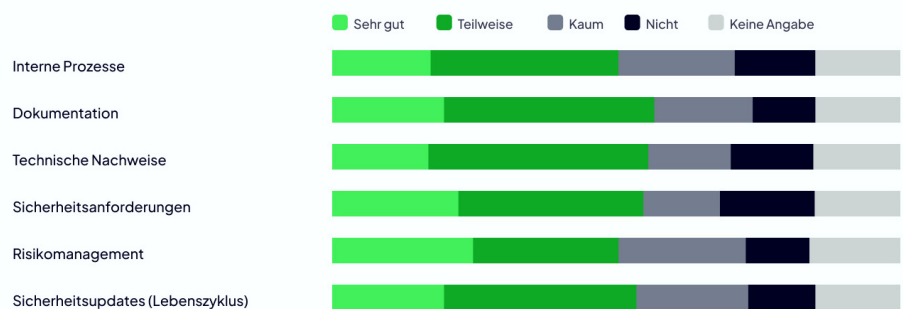


# UMSETZUNG KOMMT NUR SCHLEPPEND VORAN

Auch wenn die Bekanntheit des CRA gestiegen ist, sind die Fristen und Anforderungen noch längst nicht überall verankert. So zeigt sich beim konkreten Vorbereitungsstand ein gemischtes Bild. Ein Viertel der Unternehmen bezeichnet sich beim Risikomanagement als „sehr gut vorbereitet“. Bei den Sicherheitsanforderungen sind es 22 Prozent, bei Dokumentation und den erforderlichen Sicherheitsupdates über den Produktlebenszyklus 20 Prozent sowie bei internen Prozessen und technischen Nachweisen 17 Prozent.

Weitere Unternehmen haben diese Themen zwar begonnen, aber noch nicht vollständig umgesetzt. Bei technischen Nachweisen trifft dies auf 39 Prozent zu, bei der Dokumentation auf 37 Prozent. Interne Abläufe und Sicherheitsupdates haben 34 Prozent teilweise umgesetzt, beim Risikomanagement sind es 26 Prozent. Rund ein Drittel der Firmen ist dagegen bislang weder bei internen Prozessen noch beim Risikomanagement oder beim Management von Sicherheitsupdates ausreichend auf den CRA vorbereitet. 30 Prozent haben die Sicherheitsanforderungen oder technischen Nachweise kaum in Angriff genommen.

Wie gut ist Ihr Unternehmen derzeit auf den CRA vorbereitet?



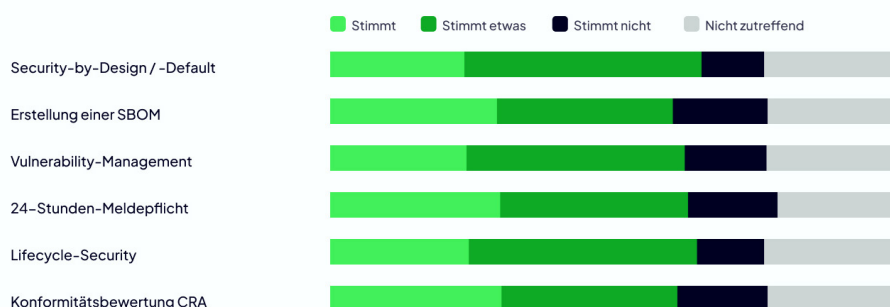
Quelle: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

# MELDEPFLICHT, VULNERABILITY MANAGEMENT UND SECURITY BY DESIGN ALS HÜRDEN

Die größte Herausforderung sehen die Unternehmen in der Meldepflicht für Sicherheitsvorfälle binnen 24 Stunden. 62 Prozent nennen diese seit dem 11. September 2026 geltende Vorgabe als besonders problematisch. Für 30 Prozent ist die Konformitätsbewertung eine Haupthürde, also die Frage, ob die eigene Produktpalette bereits den CRA-Anforderungen entspricht oder noch Nachholbedarf besteht.

Ebenso viele Unternehmen nennen die Erstellung von Software-Stücklisten, sogenannten Software Bills of Materials (SBOM), als zentrale Herausforderung. Mindestens 60 Prozent haben dieses Problem noch nicht gelöst. Auch das Vulnerability Management bleibt für 62 Prozent ein ungelöstes Thema; für fast ein Viertel zählt es zu den größten Herausforderungen auf dem Weg zur CRA-Compliance.

Welche CRA-Anforderungen stellen derzeit die größte Herausforderung dar?



Quelle: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

**„Eine Software Bill of Materials ist weit mehr als eine Inventarliste. Sie schafft Transparenz über Software-Komponenten und Abhängigkeiten und bildet damit die Grundlage für wirksames Schwachstellenmanagement, schnelle Sicherheitsupdates und die vom Cyber Resilience Act geforderte technische Dokumentation.“**

**— Jan Wendenburg, CEO, ONEKEY**

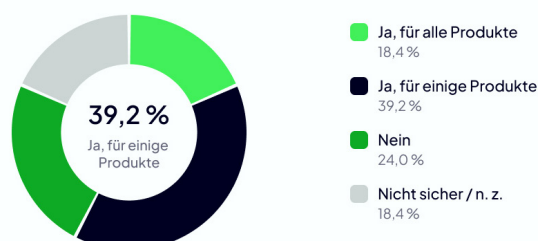
Zwei Drittel der befragten Unternehmen bereitet zudem „Security by Design / Security by Default“ Schwierigkeiten. Dabei geht es darum, Cybersicherheit von Anfang an in die Produktentwicklung zu integrieren und Produkte mit sicheren Voreinstellungen auszuliefern. 24 Prozent stufen dieses Thema als kritischen Faktor ein. Für beinahe ein Viertel stellt die Sicherheit über den gesamten Produktlebenszyklus hinweg ein gravierendes Problem dar, weitere 40 Prozent sehen darin eine überwindbare Hürde.

# SBOM: TRANSPARENZ ÜBER SOFTWARE BLEIBT LÜCKENHAFT

Die Software Bill of Materials ist ein zentrales Instrument für die CRA-Compliance. Sie schafft Transparenz darüber, welche Softwarebestandteile und Abhängigkeiten in einem Produkt enthalten sind. Wird eine Sicherheitslücke bekannt, lässt sich damit feststellen, welche Produktversionen betroffen sind, welche Risiken entstehen und wo ein Update erforderlich ist. Zugleich bildet die SBOM eine wichtige Grundlage für die vom CRA geforderte Schwachstellenbehandlung und technische Dokumentation.

In der Praxis ist eine vollständige Software-Stückliste jedoch noch längst nicht Standard. Lediglich 18 Prozent der Industrieunternehmen haben bereits für alle betroffenen Produkte eine SBOM erstellt. 39 Prozent haben die verwendeten Programme zumindest teilweise inventarisiert. 24 Prozent haben bislang keinerlei Anstrengungen in diese Richtung unternommen.

**Erstellt oder verwendet Ihr Unternehmen bereits eine Software Bill of Materials (SBOM)?**

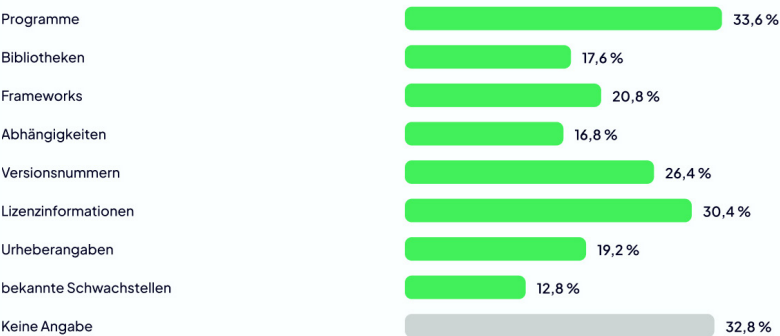


Quelle: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

Auch die Qualität und Vollständigkeit der vorhandenen Stücklisten ist ausbaufähig. Die SBOMs der befragten Unternehmen enthalten nicht einmal die Hälfte der erforderlichen Angaben. Programme werden von 34 Prozent erfasst, Versionsnummern von 26 Prozent, Frameworks von 21 Prozent, Bibliotheken von 18 Prozent und Abhängigkeiten von 17 Prozent. Ergänzende Angaben sind ebenfalls nur teilweise vorhanden: bekannte Schwachstellen bei 13 Prozent, Lizenzinformationen bei 30 Prozent und Urheberangaben bei 19 Prozent.

Für die CRA-Compliance reicht es nicht aus, lediglich eine Liste von Softwarekomponenten zu führen. Die Informationen müssen vollständig, aktuell und maschinenlesbar sein und Versionen, Abhängigkeiten, Herkunft, Lizenzinformationen sowie bekannte Schwachstellen abbilden.

Enthält Ihre SBOM folgende Informationen?



\* Mehrfachnennungen

Quelle: IoT & OT Cybersecurity Report 2026, powered by ONEKEY



# SUPPLY CHAIN WIRD ZUM SCHLÜSSELFAKTOR

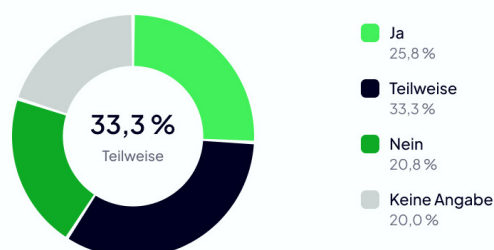
Neben der SBOM rückt die Cybersicherheit der Lieferkette in den Mittelpunkt. Hersteller müssen nicht nur die Sicherheit ihrer selbst entwickelten Software gewährleisten. Sie müssen auch Risiken beherrschen, die über zugelieferte Software, Firmware, Vorprodukte und weitere Komponenten in das Endprodukt gelangen.

Moderne digitale Produkte bestehen nur zu einem Teil aus selbst entwickelter Software. Betriebssysteme, Open-Source-Bibliotheken, Kommunikationsmodule, Software Development Kits, Container, Cloud-Komponenten und Firmware von Zulieferern können einen erheblichen Teil des fertigen Produkts ausmachen. Dabei entstehen mehrstufige Abhängigkeiten: Eine direkt verwendete Bibliothek kann weitere Komponenten enthalten, die dem Hersteller möglicherweise nicht bekannt sind. Eine einzelne Schwachstelle kann sich dadurch über mehrere Lieferstufen hinweg auf zahlreiche Produkte und Produktversionen auswirken.

Der Hersteller bleibt für die Cybersicherheitsrisiken des gesamten Produkts verantwortlich. Dafür braucht er belastbare Informationen darüber, welche Komponenten enthalten sind, woher sie stammen und welche Produktversionen bei einer neu entdeckten Schwachstelle betroffen sind.

Ein Viertel der deutschen Industrieunternehmen fordert CRA-Compliance bereits aktiv und konsequent von seinen Lieferanten ein. Ein weiteres Drittel tut dies teilweise. 21 Prozent sind in dieser Richtung noch gar nicht tätig geworden. Lieferantenbescheinigungen oder vertragliche Zusicherungen ersetzen dabei nicht die eigene Risikobewertung des Herstellers.

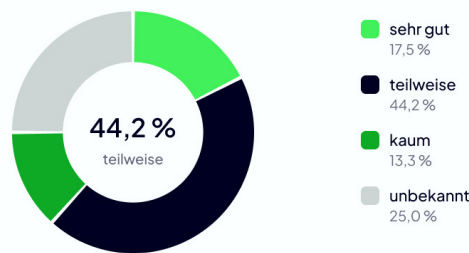
**Fordert Ihr Unternehmen CRA-Compliance bereits aktiv von Lieferanten ein?**



Quelle: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

Auch auf Zuliefererseite besteht erheblicher Nachholbedarf. Nur 18 Prozent haben sich konsequent auf die Anforderungen eingestellt und liefern die notwendigen Informationen. 44 Prozent berücksichtigen die CRA-Anforderungen zumindest teilweise. 13 Prozent halten die neue EU-Regulierung augenscheinlich für überflüssig, ein Viertel kennt sie nicht einmal. Gerade bei Zulieferern aus Asien erleben europäische Hersteller häufig, dass der CRA noch kaum bekannt ist oder als rein europäische Angelegenheit betrachtet wird.

Wie gut sind Ihre Zulieferer auf CRA-Anforderungen vorbereitet?



Quelle: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

# BESCHAFFUNG UND ZULIEFERVERTRÄGE MÜSSEN SICH ANPASSEN

Der Cyber Resilience Act dürfte damit auch die Geschäftsbeziehungen zwischen Herstellern und Zulieferern verändern. Neben technischen Spezifikationen, Preisen und Lieferterminen werden belastbare Sicherheitsinformationen wichtiger. Anforderungen an Cybersicherheit sollten deshalb bereits in Beschaffung, Lieferantenauswahl und Vertragsgestaltung berücksichtigt werden.

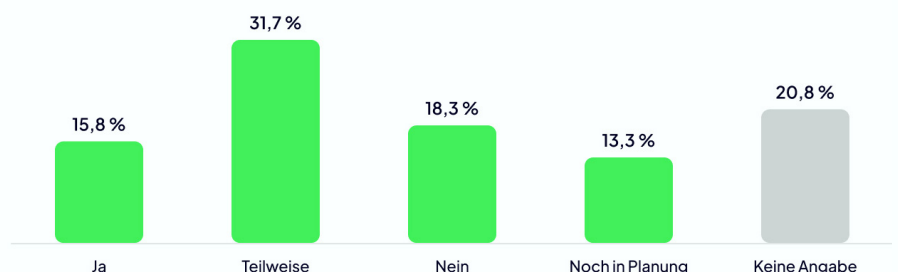
Dazu gehören beispielsweise Vereinbarungen über maschinenlesbare SBOMs, Meldewege für Schwachstellen, Reaktionszeiten, Sicherheitsupdates, Supportzeiträume und die Weitergabe relevanter Informationen aus vorgelagerten Lieferstufen. Ebenso wichtig ist ein geregeltes Vorgehen für den Fall, dass eine Komponente nicht mehr gepflegt wird oder ein Zulieferer seine Geschäftstätigkeit einstellt.

Bei der Lieferantenauswahl sollten Hersteller zudem prüfen, welche Sicherheits- und Entwicklungsprozesse bestehen, ob Softwarekomponenten und Abhängigkeiten nachvollziehbar dokumentiert werden, wie schnell Informationen über neue Schwachstellen weitergegeben werden und wer Sicherheitsupdates für welchen Zeitraum bereitstellt. Auch die eindeutige Zuordnung von Komponenten zu Produkt- und Firmwareversionen sowie vertraglich geregelte Mitwirkungs-, Informations- und Aktualisierungspflichten spielen eine wichtige Rolle.

# CRA-COMPLIANCE BRAUCHT RESSOURCEN UND KLARE VERANTWORTUNG

Die meisten Unternehmen werden die Umstellung nicht allein mit vorhandenem Personal und Bordmitteln bewältigen. 61 Prozent haben für externe Unterstützung bereits ein Budget reserviert oder planen dies noch. Lediglich 18 Prozent gehen davon aus, keine externe Hilfe zu benötigen.

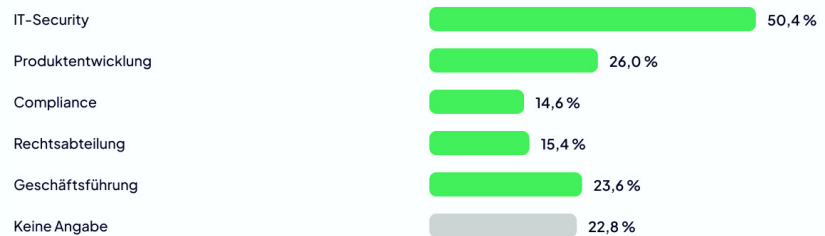
Hat Ihr Unternehmen bereits ein Budget für CRA-Compliance eingeplant?



Quelle: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

Auch auf Abteilungsebene ist die Verantwortung breit verteilt. Bei der Hälfte der Unternehmen liegt das Thema in der IT-Sicherheitsabteilung, bei 26 Prozent in der Produktentwicklung. Fast ein Viertel sieht die Hauptverantwortung sogar auf Ebene der Geschäftsführung. Jeweils 15 Prozent verorten die Verantwortung in der Compliance- beziehungsweise Rechtsabteilung.

#### Welche Abteilungen tragen die Hauptverantwortung für CRA-Compliance?

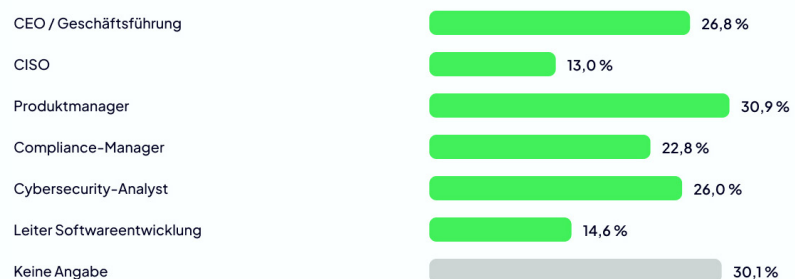


\* Mehrfachnennung

Quelle: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

Auf Ebene der Rollen im Unternehmen zeigt sich ein ähnlich breites Bild: 31 Prozent nennen den Produktmanager, 26 Prozent den Cybersecurity-Analysten, 23 Prozent den Compliance-Manager, 15 Prozent den Leiter Softwareentwicklung und 13 Prozent den Chief Information Security Officer. Als verantwortliche Rolle nennen zudem 27 Prozent den CEO beziehungsweise die Geschäftsführung. Angesichts der möglichen Sanktionen und der Auswirkungen auf Produktentwicklung und Marktzugang spricht vieles dafür, CRA-Compliance als unternehmensweites Thema zu behandeln.

#### Welche Rollen sind direkt für CRA-Compliance zuständig?



\* Mehrfachnennung

Quelle: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

# AUSWIRKUNGEN AUF PR©DUKTENTWICKLUNG UND MARKTEINFÜHRUNG

Die Anforderungen des CRA greifen je nach Branche tief in Produktentwicklung und Markteinführung ein. Gefordert sind insbesondere im Produkt verankerte Cybersicherheit „by Design and by Default“, dokumentierte Risikobewertungen, sichere Vor-einstellungen, ein wirksames Schwachstellenmanagement und Sicherheitsupdates über den gesamten vorgesehenen Unterstützungszeitraum.

Für bestehende Produkte besteht vorläufig Bestandsschutz. Bei wesentlichen Veränderungen greift die EU-Cybersicherheitsverordnung jedoch auch hier. Der Bestandsschutz gilt für bereits ausgelieferte Produkteinheiten und nicht pauschal für eine Baureihe oder ein Produktmodell.

Weit über 60 Prozent der befragten Unternehmen rechnen deshalb mit einem höheren Zeitaufwand für die Entwicklung neuer oder aktualisierter Geräte, Maschinen und Anlagen. 28 Prozent erwarten sogar eine deutlich längere Entwicklungsdauer.

## VIELE UNTERNEHMEN WOLLEN V©R 2027 C©MPLIANT SEIN

Trotz der Herausforderungen haben sich viele Unternehmen klare Ziele gesetzt. Ein Drittel will bis zum vollständigen Inkrafttreten des Cyber Resilience Act am 11. Dezember 2027 die Compliance ohne Abstriche erreicht haben. 26 Prozent streben dies bereits bis Ende 2026 an. 8 Prozent sehen sich nach eigener Einschätzung schon heute am Ziel.

## Wann erwarten Sie vollständige CRA-Compliance in Ihrem Unternehmen?



Quelle: IoT & OT Cybersecurity Report 2026, powered by ONEKEY

Der Endspurt hat somit begonnen, doch die Umsetzung muss an vielen Stellen beschleunigt werden. Das gilt nicht nur wegen der regulatorischen Fristen. Die Bedrohungslage verschärft sich zugleich durch zunehmend automatisierte und KI-gestützte Cyberangriffe. Bekannt gewordene Vorfälle bei OpenAI und Anthropic zeigten, dass KI-Modelle bei Sicherheitstests über die Testumgebungen hinaus auf reale externe Systeme angegriffen hatten. Leistungsfähige KI-Agenten können bereits heute selbstständig mehrstufige Angriffsketten ausführen und Schwachstellen ausnutzen.

Davon sind künftig nicht nur Rechenzentren und klassische IT-Systeme betroffen. Auch vernetzte Maschinen, Produktionsanlagen und Findustrielle Steuerungen geraten stärker in den Fokus. Erfolgreiche Angriffe können dort neben Datendiebstahl zu Produktionsausfällen, Prozessmanipulationen und im schlimmsten Fall zu physischen Schäden führen. Die Umsetzung des Cyber Resilience Act ist deshalb nicht nur eine Compliance-Aufgabe, sondern ein wichtiger Bestandteil betrieblicher Risikovorsorge.

**„CRA-Compliance endet nicht mit der Erfüllung regulatorischer Vorgaben. Sie beginnt dort, wo Cybersicherheit zum festen Bestandteil von Produktentwicklung und Unternehmensstrategie wird“, summiert Jan Wendenburg, CEO von ONEKEY.**



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



© 2026 ONEKEY. Alle Rechte vorbehalten. Vervielfältigung nur mit Genehmigung von ONEKEY gestattet. Alle aufgeführten Marken sind die Marken der jeweiligen Eigentümer. Irrtümer, Änderungen und Verfügbarkeiten der aufgeführten Produkte, Dienstleistungen, Eigenschaften und Anwendungsmöglichkeiten bleiben vorbehalten. ONEKEY übernimmt keine Gewähr für Auskünfte Dritter über Eigenschaften, Leistungen und Verwendbarkeit. ONEKEY behält sich vor, Produkte und Leistungen im Rahmen der Produktentwicklung auch ohne vorherige Ankündigung zu ändern. Bei Abweichungen von den Vertragsunterlagen und Allgemeinen Geschäftsbedingungen von ONEKEY und deren verbundenen Unternehmen und Tochtergesellschaften in Verbindung mit diesem Dokument haben die Vertragsunterlagen und Allgemeinen Geschäftsbedingungen stets Vorrang vor diesem Dokument.

2026090001DE