WHITEPAPER

WARUM SIE JETZT HANDELN MÜSSEN

DER EU CYBER RESILIENCE ACT (CRA)

Mit dem Cyber Resilience Act führt die Europäische Union verbindliche Anforderungen an die Sicherheit von Produkten mit digitalen Elementen ein. Erstmals wird die Cybersicherheit konsequent als wesentliche Produkteigenschaft verankert.

Die Verordnung erweitert Verantwortlichkeiten entlang des Produktlebenszyklus und der Lieferkette und stellt neue Anforderungen an Organisation, Prozesse und Produktentwicklung. Für viele Unternehmen – insbesondere kleine und mittlere – ist dies die erste regulatorische Vorgabe in diesem Umfang.

AUTOREN PROTIVITI:
ANDREJ GREINDL, CHRISTOPHER CHASSÉE, NILS VON BRINCKEN, JULIA PANZER, CAROLINE KRAFT

AUTOR ROBERT HALF:
PHILIPP WEINGART

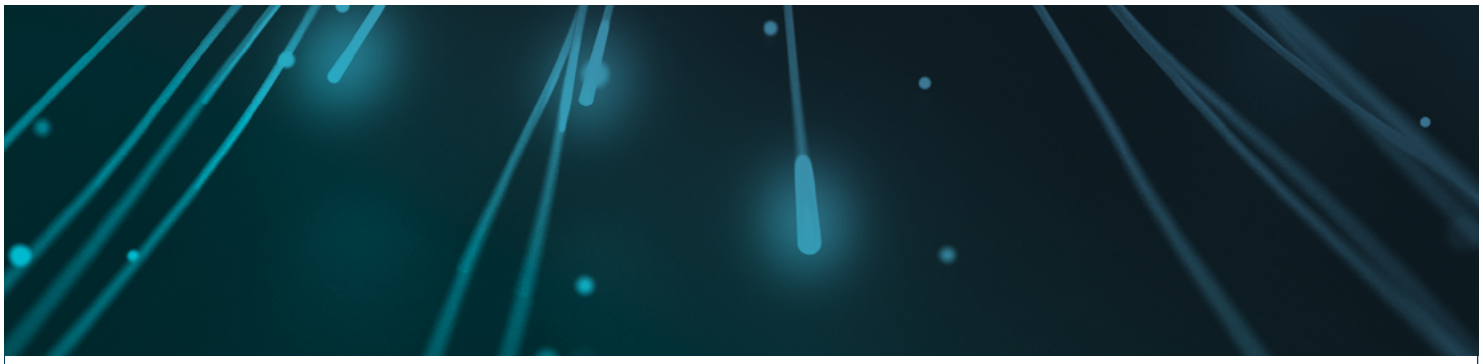
protiviti®
Global Business Consulting

Robert Half®
Talent Solutions

INHALT

protiviti® Global Business Consulting

Robert Half® Talent Solutions



1. EINLEITUNG

Die Cyberbedrohungslage in Deutschland hat sich in den vergangenen Jahren verschärft und verbleibt laut dem Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) auf einem angespannten Niveau. Cyberangriffe sind längst kein Ausnahmeereignis mehr, sondern ein wachsendes unternehmerisches Risiko mit direkten Auswirkungen auf Produktverfügbarkeit, Marktzugang und Sicherstellung der Geschäftsfortführung. Insbesondere kleine und mittelständische Unternehmen (KMU) geraten zunehmend in den Fokus von Angreifern, da sie häufig nicht über die organisatorischen, technischen und prozessualen Voraussetzungen verfügen, um Cyberrisiken systematisch zu managen [1, 2]. Parallel zu dieser Bedrohungslage hat sich die Natur von Produkten grundlegend verändert. Digitale Funktionen, Software-Komponenten und Vernetzung sind heute fester Bestandteil zahlreicher Produkte – unabhängig von Branche oder Marktsegment. Damit verlagern sich Cyberrisiken zunehmend weg vom isolierten Betrieb einzelner IT-Systeme hin zu den Produkten selbst und ihrem gesamten Lebenszyklus. Sicherheitsmängel betreffen demnach nicht mehr nur interne IT-Infrastrukturen, sondern unmittelbar die Sicherheit, Zuverlässigkeit und Konformität von Produkten am Markt. Obwohl das Thema Cyberresilienz auch für KMU nicht neu ist, stand dieser Entwicklung bislang eine fragmentierte Cybersicherheitsregulatorik auf Ebene der Europäischen Union (EU) gegenüber. Bestehende Regulatorik adressierte entweder freiwillige Produktzertifizierungen (EU Cybersecurity Act) oder den Betrieb von Netz- und Informationssystemen (NIS2-Richtlinie), jedoch nicht die Cyberresilienz digitaler Produkte über ihren gesamten Lebenszyklus hinweg. Insbesondere verbindliche Mindestanforderungen an sicheres Produktdesign, an Update- und Patchpflichten sowie an den strukturierten Umgang mit Schwachstellen und Sicherheitsvorfällen fehlten bisher.

Mit dem EU Cyber Resilience Act (CRA), dessen Anforderungen schrittweise ab 2026 zur Anwendung kommen, schließt die EU diese regulatorische Lücke und etabliert einen verbindlichen regulatorischen Rahmen für die Cybersicherheit von Produkten mit digitalen Elementen. Ziel ist es, Cybersicherheit konsequent als zentrale Produkteigenschaft zu etablieren – von der Entwicklung über das Inverkehrbringen bis hin zum Betrieb und zur Außerbetriebnahme. Betroffen sind dabei nicht nur Herstellende, sondern alle Akteure, die Produkte mit digitalen Elementen entwickeln, bereitstellen, importieren oder vertreiben [3, 4, 5].

Der CRA verschiebt Verantwortung, verändert Rollen und Prozesse und macht Cyberresilienz zu einem zentralen Kriterium für Marktzugang und Wettbewerbsfähigkeit. Wenn Sie Cyberresilienz frühzeitig strukturell in Ihrem Unternehmen verankern, schaffen Sie damit nicht nur regulatorische Sicherheit, sondern auch einen strategischen Vorteil im europäischen Binnenmarkt.

Dieses Whitepaper zeigt auf, warum eine umfassende Auseinandersetzung mit dem CRA für verantwortliche Personen erforderlich ist. Im Folgenden werden die zentralen Anforderungen zusammengefasst und typische blinde Flecken identifiziert, die insbesondere KMU berücksichtigen müssen. Ein besonderer Fokus liegt hierbei auf den Meldewegen und deren praktischer Umsetzung. Außerdem stellen wir Ihnen einen Self-Check bereit, der Sie bei der Einordnung des aktuellen Reifegrads Ihres Unternehmens in Bezug auf die CRA-Anforderungen unterstützt.

2. ANFORDERUNGEN DES CRA

Der CRA ist eine europäische Verordnung (Regulation (EU) 2024/2847), welche am 11. Dezember 2024 in Kraft trat und am 11. Dezember 2027 vollständig anwendbar sein wird. Diese Verordnung gilt für alle Produkte mit digitalen Elementen, die in der EU in Verkehr gebracht werden. Produkte gelten als solche, wenn sie direkt oder indirekt mit einem Gerät oder einem Netzwerk verbunden werden können und digitale Funktionalität besitzen. Dazu gehören sowohl vernetzte Hardware-Produkte (z. B. IoT-Geräte, smarte Systeme, industrielle Komponenten) als auch reine Softwareprodukte, die kommerziell genutzt werden (z. B. mobile Apps oder Unternehmenssoftware). Ausgenommen sind Produkte, die über weitere sektorspezifische Vorschriften reguliert sind. Eine Übersicht des Anwendungsbereiches kann der folgenden Abbildung entnommen werden.

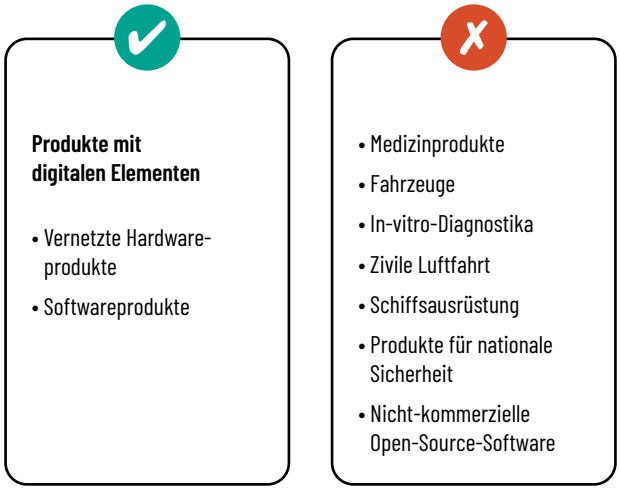


Abbildung 1: Anwendungsbereich des CRA

Da die Cybersicherheitsanforderungen über den gesamten Produktlebenszyklus erfüllt werden müssen, richtet sich die Regulatorik an ein breites Spektrum von Akteuren entlang der Lieferkette. Dazu gehören Hersteller, Importeure und Händler von Produkten mit digitalen Elementen. Die Einhaltung der Anforderungen wird in Deutschland durch das BSI überwacht. Als notifizierende und marktüberwachende Behörde kann das BSI sowohl aktiv in Form von anlasslosen Produktüberprüfungen als auch reaktiv durch entsprechende Maßnahmen tätig werden.

Durch die extraterritoriale Wirkung des CRA wird diese Verantwortung nicht auf den europäischen Binnenmarkt begrenzt, sondern auf internationale Märkte ausgeweitet und stellt somit einen Anreiz zur globalen Harmonisierung von Sicherheitsstandards dar. Zugleich werden der Binnenmarkt und das Vertrauen in Produkte auf und von dem EU-Markt gestärkt und Verbraucher werden beim Kauf und der Nutzung solcher Produkte vor Cyberbedrohungen geschützt. Vor diesem Hintergrund müssen die Akteure sicherstellen, dass die verpflichtenden Cybersicherheitsanforderungen während des gesamten Produktlebenszyklus eingehalten werden. Die Unternehmen sollten sich hierbei auf sieben Kernanforderungen konzentrieren, die im Folgenden erläutert werden [4, 5, 6].

SICHERE KONZEPTION UND ENTWICKLUNG

Produkte müssen bereits in der Entwicklungsphase so gestaltet werden, dass grundlegende Sicherheitsanforderungen erfüllt sind, bekannte Schwachstellen vermieden werden und der Einsatz veralteter oder unsicherer Komponenten ausgeschlossen ist. Dazu gehören Prinzipien wie „Security by Design“ und „Security by Default“. Hierbei muss bei der Integration von Drittanbieter-Komponenten eine ausführliche Due-Diligence-Prüfung erfolgen.

SCHWACHSTELLEN- UND VORFALLBEHANDLUNG

Die Erkennung, Bewertung und Beseitigung von Schwachstellen muss systematisch in interne Prozesse integriert und durch eine verpflichtende Dokumentation nachvollziehbar sichergestellt werden. Das Schwachstellenmanagement muss über den gesamten Supportzeitraum des Produktes betrieben werden.

SOFTWARE BILL OF MATERIALS (SBOM)

Hersteller sind verpflichtet für ihre Produkte eine Software-Stückliste (SBOM) zu erstellen. Diese dient als detaillierte Inventarliste der eingesetzten Komponenten und ist ein wesentliches Werkzeug zur Unterstützung des Schwachstellenmanagements.

KONFORMITÄTSPRÜFUNG

Bevor ein Produkt auf den Markt gebracht wird, müssen Hersteller Konformitätsbewertungsverfahren durchführen, um bei erfolgreichem Abschluss die EU-Konformitätserklärung ausstellen sowie die CE-Kennzeichnung an dem Produkt anbringen zu können.

MELDEPFLICHTEN UND MELDEWEGE

Erfasste Schwachstellen und schwerwiegende Sicherheitsvorfälle müssen über eine zentrale Meldeplattform an das nationale Computer Security Incident Response Team (CSIRT) sowie der European Union Agency for Cybersecurity (ENISA) gemeldet werden. Wie die Meldewege konkret ausgestaltet sind, wird im weiteren Verlauf dieses Whitepapers beleuchtet.

SECURITY UPDATES ÜBER LEBENSZYKLUS

Hersteller sind verpflichtet, während des Supportzeitraums ihrer Produkte regelmäßig Sicherheitsupdates bereitzustellen und eine leicht zugängliche oder automatisierte Installation zu ermöglichen. Der Supportzeitraum muss klar kommuniziert werden und spiegelt die Dauer der voraussichtlichen Nutzung des Produkts wider - mindestens jedoch fünf Jahre. Wird davon ausgegangen, dass die Nutzungsdauer des Produktes weniger als fünf Jahre beträgt, muss der Supportzeitraum der voraussichtlichen Nutzungsdauer entsprechen.

TRANSPARENZ GEGENÜBER VERBRAUCHERN

Verbraucher sind umfassend über die Cybersicherheitsfunktionen zu informieren. Das beinhaltet die Bereitstellung klarer Hinweise zu bestehenden Risiken und erforderlichen Updates, sowie entsprechende Sicherheitsinformationen in Nutzerhandbüchern zugänglich zu machen.

Die oben genannten Anforderungen sind risikobasiert und abhängig von der Produktkategorie. Je höher das Risiko in der Produktkategorie, desto strenger sind die Anforderungen und desto formaler ist die Konformitätsbewertung. Der CRA unterscheidet dabei drei Produktkategorien [4]:

- **Standardprodukte** umfassen alle Hardware- und Softwareprodukte, die digitale Funktionen enthalten (z. B. Smarte Produkte, Bildverarbeitung, Videospiele etc.). An diese Produkte werden grundlegende Sicherheitsanforderungen gestellt, die durch harmonisierte Normen vorgegeben werden. Die Konformitätsbewertung erfolgt intern durch den Herstellenden.

- **Wichtige Produkte** werden in Klasse I (Passwortmanager, Betriebssysteme etc.) und Klasse II (Firewalls, Mikroprozessoren etc.) unterteilt und erfüllen entweder zentrale Funktionen für die Cybersicherheit anderer Produkte, Netze oder Dienste oder bergen aufgrund ihrer Funktion ein erhebliches Risiko systematischer, sicherheits- oder nutzerbezogener Schäden bei Manipulation oder Missbrauch. Bei wichtigen Produkten ergeben sich zusätzliche Anforderungen an die Dokumentation, Nachweisführung und Schwachstellenbehandlung. Die Konformitätsbewertung muss teilweise extern in Form einer EU-Baumusterprüfung erfolgen.

- **Kritische Produkte** sind Produkte (z. B. Chipkarten, Smart-Meter-Gateways etc.), deren Sicherheitsmängel zu schwerwiegenden Störungen von kritischen Lieferketten im Binnenmarkt führen können oder eine kritische Abhängigkeit wesentlicher Einrichtungen von der Produktkategorie besteht. Kritische Produkte unterliegen den höchsten Cybersicherheitsanforderungen. Harmonisierte Normen sind anzuwenden und es ist entweder ein Cybersicherheitszertifikat oder eine EU-Baumusterprüfung für die Konformitätserklärung und CE-Kennzeichnung notwendig.

» Der CRA macht Cybersecurity vom „IT-Problem“ zum geschäftskritischen Steuerungsthema. Ohne klare Governance drohen nicht nur Compliance-Verstöße, sondern auch der Verlust der Marktfähigkeit. «

ANDREJ GREINDL, MANAGING DIRECTOR, PROTIVITI DEUTSCHLAND

Die folgende Abbildung zeigt eine vereinfachte und praxisorientierte Darstellung des Konformitätsbewertungsverfahrens gemäß CRA auf.

1. Produktklassifizierung

- Standardprodukt
- Wichtiges Produkt Klasse I (Anhang III)
- Wichtiges Produkt Klasse II (Anhang III)
- Kritisches Produkt

↓

2. Prüfung harmonisierter Normen

Sind harmonisierte Normen vorhanden?

- **Ja** → Anwendung möglich
- **Nein** → Alternative Konformitätsbewertung erforderlich

↓

3. Wahl des Konformitätsverfahrens

Produktklasse	Bewertungsverfahren
Standardprodukt	Interne Prüfung
Wichtig Klasse I	Interne Prüfung oder EU-Baumusterprüfung
Wichtig Klasse II	Interne Prüfung oder Cybersicherheits-Zertifikat
Kritisch	EU-Baumusterprüfung oder Cybersicherheits-Zertifikat

↓

4. Schriftliche Konformitätserklärung

✔ CE-Kennzeichnung auf Produkt anbringen

Abbildung 2: Vereinfachte Darstellung der Konformitätsbewertung

In der Praxis zeigt sich, dass der Großteil der eben dargestellten Anforderungen auf den Herstellern lastet. Hier gilt zu beachten, dass die Definition von Hersteller weit gefasst ist und nicht nur Unternehmen, die Produkte mit digitalen Elementen selbst entwickeln oder herstellen, sondern auch solche, die diese konzipieren, entwickeln oder herstellen lassen und unter eigenem Namen oder eigener Marke vermarkten als Hersteller gelten. Für die übrigen Akteure besteht die Hauptaufgabe in der sorgfältigen Due-Diligence-Prüfung entlang der Lieferkette. Importeure müssen gewährleisten, dass die Hersteller die produktbezogenen Sicherheitsanforderungen sicherstellen und das Produkt die CE-Kennzeichnung trägt. Bei Händlern umfasst die Prüfung der Anforderungserfüllung sowohl Hersteller als auch Importeure. Neben der Prüfung der CE-Kennzeichnung zählen hierzu insbesondere die Angabe der Kontaktdaten auf dem Produkt, die Angabe des Supportzeitraums sowie die Bereitstellung von Sicherheitsinformationen für Verbraucher. Kommen die Akteure ihren Pflichten nicht nach, werden Verstöße gegen den CRA mit Geldbußen von bis zu:

- 15 Millionen Euro oder
- 2,5 % des weltweiten Jahresumsatzes

geahndet. Außerdem müssen die jeweiligen Produkte vom Markt genommen werden [3, 4].

3. ZENTRALE HERAUSFORDERUNGEN FÜR KMU

Der CRA konfrontiert insbesondere KMU mit organisatorischen, technischen und regulatorischen Herausforderungen – für viele Unternehmen stellt der CRA die erste umfassende Regulatorik dieser Art dar. Während Ziel und Umfang der Verordnung klar definiert sind, ergeben sich vor allem aus begrenzten finanziellen und personellen Ressourcen, komplexen Lieferkettenstrukturen und bislang wenig etablierten bzw. formalisierten Sicherheits- und Compliance-Prozessen häufig Unsicherheiten bei den verantwortlichen Personen in KMU.

In der Praxis erschwert die Nutzung von Drittanbieter-Software- und Hardwarekomponenten die klare Abgrenzung von Verantwortlichkeiten und Rollen entlang der Lieferkette. Fehlende Transparenz über eingesetzte Drittkomponenten, deren

Sicherheitsstatus und Wartungszyklen beeinträchtigen die Fähigkeit, Risiken entlang der Lieferkette angemessen zu bewerten. Die Weitergabe von Pflichten innerhalb der Lieferkette oder ein Rollenwechsel, etwa wenn Händler in Bezug auf ein Produkt Funktionen von Herstellern übernehmen, führen häufig zu unklaren Verantwortlichkeiten im Kontext der Sicherheit und Konformität des Endprodukts [3].

Des Weiteren ergeben sich aus den zuvor genannten Kernanforderungen des CRA erhebliche ressourcenbezogene Herausforderungen für KMU. Trotz begrenzter Ressourcen sind neue Prozesse und Strukturen erforderlich, um die regulatorischen Vorgaben systematisch und in der notwendigen Tiefe umzusetzen. Die kontinuierliche Überwachung, Bewertung und Behebung von Sicherheitslücken über den gesamten Produktlebenszyklus binden dabei dauerhaft Ressourcen. Punktuelle Einzelmaßnahmen reichen unter diesen Bedingungen nicht aus; vielmehr ist ein systematischer Ansatz mit etablierten Prozessen und einem hohen technologischen Reifegrad erforderlich. Zugleich stehen die Unternehmen unter hohem Innovationsdruck, wodurch die sicheren Entwicklungsprozesse im Spannungsfeld zur schnellen Produktentwicklung stehen.

Diese Aufwendungen werden häufig unterschätzt, da ihre Auswirkungen nicht unmittelbar mit Einführung der Regulatorik sichtbar sind, sondern sich erst im Rahmen von Sicherheitsvorfällen, Haftungsfragen oder regulatorischen Prüfungen konkretisieren. Dabei stellen sie einen signifikanten organisatorischen Mehraufwand dar, der eher frühzeitig adressiert werden muss. Die Wiederverwendung von bestehenden Strukturen aus anderen Regulierungen und Etablierung von Managementsystemen kann hier die Compliance unterstützen.

Auch wenn das BSI die KMU bei der Umsetzung der regulatorischen Anforderungen durch Leitlinien und Helpdesks unterstützt [5] stehen die Unternehmen jetzt sowohl in der regulatorischen Compliance als auch im Hinblick auf technologische Entwicklungen großen Herausforderungen gegenüber. Diese Effekte addieren sich insbesondere bei Meldepflichten durch weitere Regulierungen wie beispielsweise den EU AI Act, NIS2 oder die DSGVO. Vor diesem Hintergrund rückt die Umsetzung der Meldewege im CRA in den Fokus, worauf im Folgenden detailliert eingegangen wird.

4. VERTIEFUNG: MELDEWEGE IM CYBER RESILIENCE ACT

Mit dem CRA führt die EU ab dem 11. September 2026 ein Meldeverfahren ein, das über bloße technische Vorfälle hinausgeht und die Sicherheit digitaler Produkte als fortlaufende Verpflichtung in den Mittelpunkt stellt. Für Hersteller und Anbieter bedeutet dies, dass sie nicht nur über Risiken nachdenken müssen, sondern auch darüber, wie potenzielle Sicherheitsprobleme institutionell verankert erfasst und kommuniziert werden.

Zentraler Ankerpunkt dieses Prozesses ist eine neue EU-weite Meldeinfrastruktur, die von der ENISA eingerichtet wird: die Single Reporting Platform (SRP). Über diese Plattform sollen künftige Meldungen zu sicherheitsrelevanten Ereignissen für Produkte mit digitalen Elementen abgegeben werden. Damit wird erstmals ein Meldeweg etabliert, der über nationale Grenzen hinausgeht und den Austausch zwischen Herstellern, nationalen Sicherheitsteams (CSIRTs) und EU-Behörden strukturiert [7].

Der CRA strukturiert das Meldeverständnis in zeitlich gestaffelte Phasen, die sich nicht an starren Bürokratiezyklen orientieren, sondern an der Dynamik realer Sicherheitsrisiken:

1. Erste Hinweise innerhalb von 24 Stunden

Sobald ein Unternehmen von einer kritischen oder aktiv ausgenutzten Schwachstelle oder einem schwerwiegenden Sicherheitsvorfall erfährt, ist eine erste Information darüber zeitnah über die SRP zu übermitteln. Dieser frühe Schritt dient weniger der Detailanalyse als vielmehr der Frühwarnung. Es soll ein Signal sein, das Behörden und andere potenziell Betroffene dieser Schwachstelle schnell auf potenzielle Risiken aufmerksam macht. Somit können bei Bedarf länderübergreifend andere Akteure informiert werden.

2. Vertiefende Meldung nach Analyse innerhalb von 72 Stunden

Im Anschluss muss eine detaillierte Bewertung, einschließlich der Meldung, erfolgen, die den Kontext, erste Einschätzungen zur Wirkung und die Einordnung in Produktgruppen beschreibt. Diese Phase spiegelt wider, dass Sicherheit nicht allein ein technisches Ereignis, sondern ein vernetzter Sachverhalt ist, der Entwicklung, Betrieb und Nutzen für alle Beteiligten umfasst.

3. Finaler Abschlussbericht innerhalb von 14 Tagen
Sobald sich die Lage geklärt hat und erste Maßnahmen ergriffen wurden, dient ein abschließender Bericht dazu, die Beobachtungen zu konsolidieren und Lehren für künftige Bedrohungen und Risiken zu ziehen. Damit bietet der Meldeweg auch eine lehrende Komponente – er ist weniger ein administrativer Endpunkt als ein Bestandteil eines kontinuierlichen Sicherheitsprozesses.

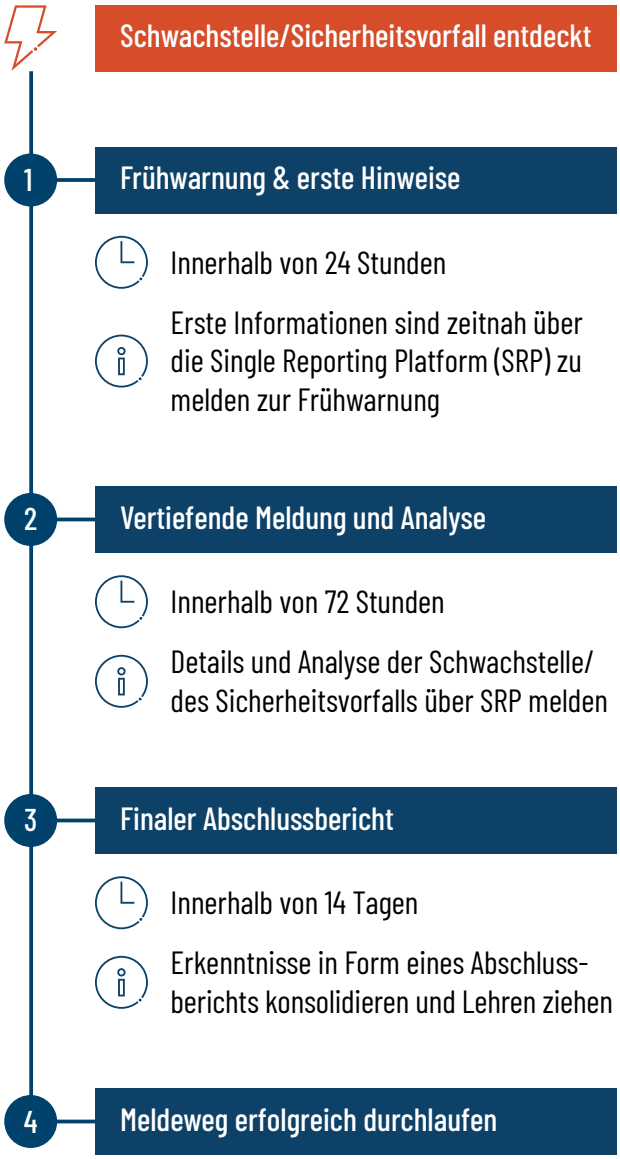


Abbildung 3: Meldeweg des CRA

Diese Stufen zeigen, dass der CRA Meldepflichten nicht als bürokratische Pflicht vorsieht, sondern als moderiertes Informations- und Steuerungsinstrument [4, 7]. Davon profitieren nicht nur die direkt Beteiligten, sondern auch andere Hersteller und Nutzer ähnlicher Produkte. Diese werden auf die Schwachstellen hingewiesen und können rechtzeitig Updates zur Verfügung stellen bzw. gestellt bekommen.

Der eigentliche Mehrwert liegt weniger im Einhalten von Fristen als in der Etablierung eines gemeinsamen Verständnisses von Risiko und Reaktion.

Die Entscheidung Meldungen über eine zentrale EU-Plattform zu kanalisieren, ist kein technokratischer Detailpunkt, sondern Ausdruck eines Paradigmenwechsels. Statt in jedem Mitgliedstaat einzeln zu melden, nutzen Hersteller eine gemeinsame Meldeinstanz, die übergreifend koordiniert:

- Hersteller reichen einen Bericht über die SRP ein
- Nationale CSIRTs werden informiert und können länderübergreifend reagieren
- ENISA aggregiert, analysiert und erleichtert Informationsaustausch

Für KMU bedeutet dies: Sie müssen sich nicht auf unterschiedliche Meldewege in verschiedenen Ländern einstellen, sondern auf einen einheitlichen, gemeinsamen Informationsraum.

Wesentlich für das Verständnis des Meldewegs im CRA ist der Blick auf die Regulatorik-Landschaft insgesamt: Meldepflichten existieren nicht isoliert. Bereits heute sehen andere Regelwerke Meldeprozesse vor, die sich inhaltlich und zeitlich mit den Anforderungen des CRA überlappen oder ergänzen, wobei die folgenden Beispiele nur Auszüge darstellen und keinen vollständigen Überblick über die entsprechenden Meldewege geben.

Die DSGVO fordert die Meldung von Datenschutzverletzungen, wenn ein Risiko für betroffene Personen vorliegt. Im Finanzbereich verlangt DORA die Meldung von ICT-Incidents, die für kritische und wichtige Dienste relevant sind. Die NIS-2-Richtlinie erweitert die Anforderungen an das Incident Reporting für eine Vielzahl von Einrichtungen erheblich und verschärft Fristen sowie Governance-Vorgaben. Auch der EU AI Act wird Meldepflichten für schwerwiegende KI-bezogene Vorfälle vorsehen.

Das Ergebnis ist eine kumulierende Erwartung an Unternehmen, mehrere Meldewege gleichzeitig zu verstehen und zu bedienen.

Für viele KMU führt dies zu Unklarheiten darüber, welches Ereignis nach welcher Regulatorik gemeldet werden muss. Hier liegt ein zentraler praktischer wie strategischer Schmerzpunkt: Wenn Meldepflichten getrennt von den zugrunde liegenden Prozessen betrachtet werden, entstehen Silos, Doppelmeldungen und Reaktionsverzögerungen.

Für KMU ist nicht allein das Einhalten einzelner Fristen entscheidend, sondern die Prozessverankerung von Meldungs- und Reaktionslogiken im Unternehmen. Es benötigt einen internen Incident-Managementprozess, welcher Verantwortlichkeiten festlegt, Ereignisse früh erkennt, bewertet und strukturiert aufzubereiten weiß. Ein solcher Ansatz entlastet zugleich im Kontext anderer Regulatorien und macht Meldepflichten zu einem integralen Teil der Sicherheits- und Risikosteuerung. Wer regulatorische Anforderungen übergreifend denkt, reduziert Komplexität und stärkt zugleich seine organisatorische Reife.

Unterstützung bei dem beschriebenen Meldeweg liefern der CRA selbst sowie die Technische Richtlinie (TR)-03183 des BSI [8, 9]. Insbesondere in der Technischen Richtlinie kann nachgelesen werden, wie Hersteller ihrer Pflicht nachgehen können ihre Kunden zu informieren.

5. SELF-CHECK: IST IHR UNTERNEHMEN AUF DEN CRA VORBEREITET?

Der CRA stellt keine klassische Compliance-Checkliste dar, sondern wirkt sich tief auf die Produktentwicklung, Organisation und Governance aus.

Die folgenden Fragen sollen Ihnen dabei helfen, den eigenen Handlungsbedarf realistisch einzuschätzen. Sie ersetzen keine formale Bewertung – zeigen jedoch, wo blinde Flecken existieren und Risiken entstehen können.

1. Klarheit über Betroffenheit & Produkte

- Haben Sie vollständig identifiziert, welche Ihrer Produkte unter den CRA fallen?
- Ist Ihnen bekannt, welche Software- und Hardware-Komponenten (inkl. Open Source) in diesen Produkten enthalten sind?
- Wissen Sie, welche Pflichten sich aus Ihrer Betroffenheit konkret für Ihr Unternehmen ergeben?

Reflexion: Unklare Betroffenheit führt in der Praxis häufig dazu, dass notwendige Maßnahmen zu spät oder unvollständig umgesetzt werden.

2. Security in der Produktentwicklung

- Sind Sicherheitsanforderungen verbindlicher Bestandteil Ihres Entwicklungsprozesses?
- Wird Security bereits in der Design-Phase berücksichtigt?
- Gibt es klare Kriterien, wann ein Produkt als „sicher genug“ gilt?
- Werden sicherheitsrelevante Entscheidungen nachvollziehbar dokumentiert?

Reflexion: Der CRA verschiebt den Fokus von reaktiver Absicherung hin zu „Security by Design“ und „Security by Default“. Unternehmen ohne strukturierte Entwicklungsprozesse stehen hier oft vor grundlegenden Anpassungen.

3. Umgang mit Schwachstellen & Updates

- Existiert ein definierter Prozess für den Umgang mit Schwachstellen über den gesamten Produktlebenszyklus?
- Werden Sicherheitsupdates zeitnah und zuverlässig bereitgestellt?
- Ist klar geregelt, wer Schwachstellen bewertet, priorisiert und allgemein verantwortet?
- Wissen Sie, wie Sie im Falle einer aktiv ausgenutzten Schwachstelle reagieren müssen?

Reflexion: Viele Organisationen haben technische Lösungen – aber keine klaren Verantwortlichkeiten. Genau hier entstehen im Ernstfall erhebliche Risiken.

4. Organisation, Rollen & Governance

- Sind Verantwortlichkeiten für CRA-relevante Themen eindeutig definiert?
- Arbeiten Produktmanagement, Entwicklung, Security und Legal strukturiert zusammen?
- Ist das Thema CRA auf Management-Ebene verankert?

Reflexion: Der CRA ist kein reines IT-Thema. Ohne übergreifende Governance-Struktur lassen sich die Anforderungen kaum nachhaltig erfüllen.

5. Dokumentation, Nachweisfähigkeit & Marktaufsicht

- Können Sie Ihre Sicherheitsmaßnahmen gegenüber Behörden und Kunden nachvollziehbar darlegen?
- Existiert bereits technische Dokumentation, die die CRA-Anforderungen angemessen berücksichtigt?
- Sind Sie vorbereitet auf Rückfragen von Marktaufsichtsbehörden?
- Wissen Sie, welche Nachweise Sie im Zweifel vorlegen müssen?

Reflexion: Nicht die fehlende Sicherheit, sondern die fehlende Nachweisfähigkeit wird häufig zur Herausforderung.

Einordnung der eigenen Situation

Wenn Sie mehrere Fragen:

- Mit „**Nein**“ beantwortet haben → akuter Handlungsbedarf
- Mit „**Teilweise**“ beantwortet haben → strukturelle Lücken
- Mit „**Ja**“ beantwortet haben → gute Ausgangsbasis, aber mutmaßlich Detailarbeit notwendig

Der CRA verlangt keine Perfektion, aber nachvollziehbare, belastbare Strukturen.

In der praktischen Umsetzung sehen wir, dass Unternehmen selten an einzelnen technischen Maßnahmen scheitern, sondern an fehlender Transparenz, unklaren Verantwortlichkeiten und fehlender Gesamtarchitektur. Zudem beobachten wir, dass die größte Herausforderung bei der CRA-Umsetzung in der nachhaltigen organisatorischen Verankerung liegt. Viele Unternehmen müssen zunächst ein geeignetes Managementsystem etablieren, das klare Verantwortlichkeiten, Entscheidungswege und Kontrollmechanismen schafft. Ohne diese Grundlage bleibt Cybersecurity häufig ein Querschnittsthema, das zwischen Entwicklung, Produktmanagement und Compliance verteilt ist, mit dem Risiko, dass Maßnahmen punktuell umgesetzt werden, jedoch keine konsistente Gesamtsteuerung entsteht.

Zudem sehen wir, dass die Interpretation der CRA-Vorgaben in vielen KMU Unsicherheit auslöst. Anforderungen wie Security-by-Design oder die Verpflichtungen rund um das Schwachstellenmanagement lassen Spielräume offen, die stark vom Produktportfolio und dem jeweiligen Risikoprofil abhängen. Gleichzeitig ist es für KMU schwierig, den tatsächlichen regulatorischen Druck realistisch einzuschätzen, auch weil in vielen Fällen noch Unklarheit darüber besteht, welche Stellen künftig als notifizierende Entitäten auftreten und wie konkret die Konformitätsbewertung in der Praxis ausgestaltet sein wird. Diese Unsicherheit kann dazu führen, dass Umsetzungsinitiativen verzögert werden.

Ein weiterer kritischer Punkt ist die Entwicklung, Anpassung und Dokumentation relevanter Prozesse. Der CRA verlangt nicht nur technische Sicherheitsmaßnahmen, sondern vor allem nachvollziehbare Nachweise über den gesamten Produktlebenszyklus hinweg. Viele Unternehmen unterschätzen dabei den Aufwand, Entwicklungs-, Change- und Incident-Managementprozesse so weiterzuentwickeln, dass sie operativ effizient und wirksam durchgeführt werden können.

» Unternehmen, die frühzeitig mit Pilotprojekten starten, gewinnen nicht nur regulatorische Sicherheit – sie schaffen auch intern ein gemeinsames Verständnis für Produktsicherheit, das langfristig Innovation beschleunigt. «

CHRISTOPHER CHASSÉE, DIRECTOR, PROTIVITI DEUTSCHLAND

Des Weiteren fordert der CRA in vielen Organisationen eine kulturelle Entwicklung. Häufig ist noch nicht ausreichend Awareness vorhanden, um Cybersecurity als festen Bestandteil von Produktqualität und Unternehmensverantwortung zu verankern. Erfolgreiche Umsetzung bedeutet daher auch, interne Akzeptanz zu schaffen und Sicherheit als kontinuierlichen Prozess zu etablieren.

Es zeigt sich, dass Unternehmen, die mit der Umsetzung der Anforderungen des CRA pragmatisch starten und die Prozesse iterativ weiterentwickeln, meist schneller messbare Fortschritte erzielen als solche, die aufgrund der Komplexität zunächst in Analysephasen verharren. Eine strukturierte CRA-Reifegrad-Analyse hilft dabei, Risiken frühzeitig zu erkennen, Maßnahmen zu priorisieren und den CRA pragmatisch umzusetzen. Entscheidend ist, frühzeitig Klarheit zu schaffen, bevor regulatorischer Druck oder Sicherheitsvorfälle zum Treiber werden.

6. STRATEGISCHE UMSETZUNG DES CRA ALS WETTBEWERBSVORTEIL

Für Hersteller, Importeure und Händler von Produkten mit digitalen Komponenten stellt sich längst nicht mehr die Frage der Betroffenheit, sondern die der strukturierten Umsetzung des CRA. Der CRA schafft einen verbindlichen europäischen Rahmen für Cybersicherheitsanforderungen über den gesamten Produktlebenszyklus hinweg. Damit entsteht nicht nur Regulierung, sondern vor allem Klarheit: Anforderungen sind definiert, Verantwortungen benannt und Erwartungen transparent formuliert.

Diese Klarheit ist ein zentraler Vorteil. Unternehmen erhalten einen belastbaren Orientierungsrahmen, an dem sie ihre Produktentwicklung und interne Prozesse ausrichten können. Wer Sicherheitsanforderungen frühzeitig integriert, profitiert doppelt. „Security by Design“ reduziert langfristig technische Schulden und vermeidet kostenintensive Nachbesserungen in späten Entwicklungsphasen. Gleichzeitig erhöht ein strukturierter Umgang mit Schwachstellen, Updates und Dokumentation die Stabilität und Qualität von Produkten. Sicherheit entwickelt sich damit vom reaktiven Aufwandstreiber zu einem festen Bestandteil der Produktstrategie.

Auch im Vertriebskontext entfaltet die Umsetzung der Forderungen des CRA positive Effekte. Kunden und Geschäftspartner erwarten zunehmend nachvollziehbare Sicherheitsstandards und transparente Prozesse.

Unternehmen, die hier belastbare Strukturen, klare Dokumentation und definierte Meldewege vorweisen können, stärken Vertrauen und Reputation nachhaltig. Gerade für KMU eröffnet sich die Chance, sich als professioneller und verlässlicher Anbieter zu positionieren. Insbesondere in regulierten oder sicherheitskritischen Branchen lassen sich durch die Synergien zwischen den Anforderungen verschiedener Regulierungen zusätzliche Effizienzgewinne erzielen.

» Durch die frühzeitige Festlegung klarer Prioritäten und die Entwicklung einer CRA-Roadmap können Unternehmen nicht nur regulatorische Risiken reduzieren, sondern sich auch messbare Wettbewerbsvorteile im EU-Markt sichern. «

PHILIPP WEINGART, DISTRICT DIRECTOR, ROBERT HALF

Darüber hinaus führt die Umsetzung häufig zu einer spürbaren Professionalisierung interner Abläufe. Risikoanalysen werden systematischer durchgeführt, Verantwortlichkeiten klar geregelt und Entscheidungswege transparenter dokumentiert. Diese erhöhte Prozessreife verbessert nicht nur die Compliance-Fähigkeit, sondern steigert insgesamt die Steuerungs- und Innovationsfähigkeit des Unternehmens. Einheitliche Sicherheitsstandards entlang der Lieferkette schaffen zusätzliche Stabilität und reduzieren Abstimmungsrisiken mit Zulieferern. Die Umsetzung der Forderungen des CRA ist damit weit mehr als eine regulatorische Pflichtübung – sie ist ein strategischer Hebel für Qualität, Vertrauen und nachhaltige Marktpositionierung.

7. FAZIT

Die Umsetzung der CRA-Anforderungen ist anspruchsvoll. Sie erfordert eine juristisch und fachlich korrekte Interpretation der Vorgaben, eine technisch fundierte Implementierung sowie die enge Verzahnung von Entwicklung, IT-Sicherheit, Recht und Management. Insbesondere für KMU können begrenzte Ressourcen und fehlendes spezialisiertes Knowhow eine Herausforderung darstellen.

Gleichzeitig liegt genau hier die Chance. Unternehmen, die CRA-Compliance als strategisches Organisationsprojekt begreifen, erhöhen ihre Prozessreife und positionieren sich langfristig wettbewerbsfähig im europäischen Markt. Entscheidend ist, frühzeitig die richtigen Prioritäten zu setzen und regulatorische Anforderungen strukturiert zu integrieren.

Der CRA setzt den Rahmen, die konkrete Ausgestaltung entscheidet über den Mehrwert. Mit einer klaren Roadmap, pragmatischen Maßnahmen und Vorgehensweisen und einer zielgerichteten Priorisierung lassen sich regulatorische Anforderungen in nachhaltige Wettbewerbsvorteile überführen.

Wenn Sie die Umsetzung des CRA gezielt gestalten wollen, begleiten wir von Protiviti Sie gerne bei der strukturierten Analyse, der Definition praktikabler Maßnahmen und der nachhaltigen Integration in Ihre Organisation. Außerdem kann Robert Half Sie dabei unterstützen kurzfristig passgenaue Ressourcen für die Umsetzung der Anforderungen des CRA zu finden. Unser Anspruch ist es, regulatorische Sicherheit mit unternehmerischem Mehrwert zu verbinden. Kontaktieren Sie uns gerne!

8. QUELLEN

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.) (2025). Die Lage der IT-Sicherheit in Deutschland 2025. https://medien.bsi.bund.de/lagebericht/Lagebericht2025_Achtseiter.pdf (Zugriff 07/2026)

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.) (2024). Cybersicherheit für KMU. Die TOP 14 Fragen. 3. Auflage. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Cybersicherheit_KMU.html (Zugriff 07/2026)

[3] Engels, B., Lang, T., & Scheufen, M. (2025). KI-Verordnung, NIS 2 Richtlinie und Cyber Resilience Act: Auswirkungen auf KMU (Kurzstudie). Ramboll Management Consulting GmbH in Zusammenarbeit mit Institut der deutschen Wirtschaft Köln e. V. und IW Consult GmbH. https://www.mittelstand-digital.de/MD/Redaktion/DE/Publikationen/kurzstudie-ki-verordnung.html (Zugriff 07/2026)

[4] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), OJ L 327, 20.11.2024, pp. 1–ff. (text with EEA relevance). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847 (Zugriff 07/2026)

[5] Bundesamt für Sicherheit in der Informationstechnik (BSI). (o. J.). Cyber Resilience Act. BSI. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act.html (Zugriff 07/2026)

[6] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.) (2026). Cyber Resilience Act: BSI wird marktüberwachende Behörde. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/251007_CRA_BSI_marktueberwachende_Behoerde.html (Zugriff 07/2026)

[7] European Commission (Hrsg.) (2026). Cyber Resilience Act - Reporting obligations. https://digital-strategy.ec.europa.eu/en/policies/cra-reporting (Zugriff 07/2026)

[8] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.) (2026). BSI TR-03183 Cyber-Resilienz-Anforderungen.
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03183/TR-03183_node.html (Zugriff 07/2026)

[9] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.) (2026). CRA-Konformität: BSI startet Kommentierungsphase für TR-03183-H.
https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/2026/Kommentierungsphase_TR-03183-H_260227.html (Zugriff 07/2026)

ÜBER PROTIVITI

Protiviti *(www.protiviti.com)* ist ein weltweit tätiges Beratungsunternehmen, das fundiertes Fachwissen, objektive Erkenntnisse, einen maßgeschneiderten Ansatz und beispiellose Zusammenarbeit bietet, um Führungskräfte selbstbewusst in die Zukunft blicken zu lassen. Protiviti und seine unabhängigen und regional ansässigen Mitgliedsfirmen unterstützen Kunden mit Beratungsleistungen und Managed Solutions in Bezug auf Finanzen, Technologien, Operatives, Digitales, HR, Risiko und Interne Revision – mithilfe eines Netzwerkes von mehr als 90 Niederlassungen in über 25 Ländern.

Protiviti wurde zum zehnten Mal in Folge in die Liste der **Fortune 100 Best Companies to Work For®** aufgenommen und hat mehr als 80 Prozent der Fortune-100- und fast 80 Prozent der Fortune-500-Unternehmen betreut. Protiviti arbeitet ebenfalls mit Regierungsbehörden sowie kleineren und wachsenden Unternehmen zusammen, einschließlich solchen, die den Börsengang planen. Protiviti ist darüber hinaus eine hundertprozentige Tochter der **Robert Half Inc.** (NYSE: RHI).

www.protiviti.de

protiviti® Global Business Consulting

Robert Half® Talent Solutions

9. IHRE KONTAKTE BEI PROTIVITI UND ROBERT HALF

ANDREJ GREINDL
Managing Director Tech-Audit
Protiviti Deutschland
andrej.greindl@protiviti.com

CHRISTOPHER CHASSÉE
Director Technology Risk & Resilience
Protiviti Deutschland
christopher.chassee@protiviti.com

PHILIPP WEINGART
District Director
Robert Half
philipp.weingart@roberthalf.de

NILS VON BRINCKEN
Manager Technology Risk & Resilience
Protiviti Deutschland
nils.vonbrincken@protiviti.com

JULIA PANZER
Consultant Technology Risk & Resilience
Protiviti Deutschland
julia.panzer@protiviti.com

CAROLINE KRAFT
Consultant Technology Risk & Resilience
Protiviti Deutschland
caroline.kraft@protiviti.com