orka Newsletter | IT-, KI- & Datenrecht

Cyber Resilience Act –Meldepflichten ab September 2026

Ab dem 11. September 2026 müssen Hersteller von Produkten mit digitalen Elementen Sicherheitsschwachstellen und schwerwiegende Sicherheitsvorfälle an die zuständigen Behörden melden. Die **neuen Meldepflichten des Cyber Resilience Act (CRA)** treten damit deutlich vor den übrigen Vorgaben der Verordnung in Kraft – und betreffen auch bereits auf dem Markt befindliche Produkte.

Dieser Newsletter gibt einen **Überblick über die wesentlichen Anforderungen** und zeigt, welche Schritte Hersteller jetzt einleiten sollten.

Was regelt der CRA?

Die Verordnung (EU) 2024/2847 – bekannt als Cyber Resilience Act (CRA) – legt horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen fest und ergänzt damit den bestehenden Rechtsrahmen der Union auf dem Gebiet der Cybersicherheit.

Hintergrund des CRA ist die Feststellung der EU, dass Cybersicherheitsvorfälle – darunter solche, die auf die Ausnutzung von Schwachstellen in Hardware- und Softwareprodukten zurückzuführen sind – der Gesellschaft und Wirtschaft der Union erhebliche Schäden zufügen. Viele dieser Schwachstellen sind auf mangelhafte Sicherheit bereits in der Entwurfsphase sowie auf fehlende Sicherheitsaktualisierungen zurückzuführen.

Der CRA gilt für **„Produkte mit digitalen Elementen"**, d.h. Software- und

Hardwareprodukte und ihre Fernverarbeitungslösungen für Daten, einschließlich Software- oder Hardwarekomponenten, die separat in Verkehr gebracht werden.

Zentrale Voraussetzung für die Einbeziehung in den Anwendungsbereich des CRA ist, dass der bestimmungsgemäße Verwendungszweck oder die vernünftigerweise vorhersehbare Verwendung des Produkts eine **Datenverbindung mit einem anderen Gerät oder einem Netz** umfasst. Entscheidend ist dabei, dass keine Internetverbindung im engeren Sinne erforderlich ist: Auch Produkte, die ausschließlich eine lokale oder physische Verbindung herstellen – etwa über Bluetooth, USB oder eine Nahfeldkommunikation – können in den Anwendungsbereich fallen.

Zu den vom CRA erfassten Produktarten zählen unter anderem eigenständige Software (z. B. Desktop-Anwendungen oder mobile Apps), Firmware und eingebettete Software, Hardware-Software-Kombinationen sowie Hardwareprodukte wie Router, Smartphones, Smart-Home-Geräte oder industrielle IoT-Geräte.

Der CRA richtet sich nicht ausschließlich an Hersteller. Er erfasst **sämtliche Wirtschaftsakteure**, die in der Liefer- und Vertriebskette von Produkten mit digitalen Elementen tätig sind (z.B. Importeure und Händler) – mit abgestuften Pflichten je nach Rolle.

Meldepflichten für Hersteller ab 11. September 2026

Während der CRA grundsätzlich erst ab dem 11. Dezember 2027 gilt, treten die **Meldepflichten des Artikels 14 bereits ab dem 11. September 2026** in Kraft.

Diese Vorverlagerung betrifft nicht nur neue Produkte: Abweichend von den allgemeinen Übergangsbestimmungen gelten die Meldepflichten des Artikels 14 **für alle Produkte** mit digitalen Elementen im Anwendungsbereich des CRA – auch für Produkte, die vor dem 11. Dezember 2027 auf dem Markt bereitgestellt wurden.

Für Hersteller bedeutet dies in der Praxis: Die Meldepflicht gilt für ihr **gesamtes aktuelles Produktportfolio** – unabhängig davon, wann das jeweilige Produkt entwickelt wurde und in Verkehr gebracht worden ist. Eine Ausnahme von dieser Verpflichtung besteht nicht.

Artikel 14 CRA verpflichtet Hersteller zur Meldung von zwei voneinander unabhängigen Ereigniskategorien:

„Aktiv ausgenutzte Schwachstellen“

Eine „aktiv ausgenutzte Schwachstelle" ist eine Schwachstelle, zu der verlässliche Nachweise dafür vorliegen, dass ein **böswilliger Akteur** sie in einem System ohne Zustimmung des Eigentümers dieses Systems ausgenutzt hat.

Für die Praxis konkretisiert der CRA den Begriff dahingehend, dass eine aktiv ausgenutzte Schwachstelle dann vorliegt, wenn der Hersteller feststellt, dass eine Sicherheitsverletzung, die sich auf seine Nutzer oder andere natürliche oder juristische Personen auswirkt, darauf zurückzuführen ist, dass ein böswilliger Akteur einen Fehler in einem der vom Hersteller auf dem Markt bereitgestellten Produkte ausnutzt.

„Schwerwiegende Sicherheitsvorfälle“

Ein Sicherheitsvorfall mit Auswirkungen auf die Sicherheit eines Produkts mit digitalen Elementen gilt als **„schwerwiegend"**, wenn er (i) die Fähigkeit des Produkts, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit sensibler oder wichtiger Daten oder Funktionen zu schützen, negativ beeinträchtigt oder beeinträchtigen kann, oder wenn er (ii) zur Einführung oder Ausführung eines böswilligen Codes in einem Produkt oder im Netz- und Informationssystem eines Nutzers geführt hat oder führen kann.

Der Begriff des schwerwiegenden Sicherheitsvorfalls ist bewusst weit gefasst. Es genügt, dass der Vorfall die Produktsicherheit **beeinträchtigen kann** – ein tatsächlich eingetretener Schaden bei Nutzern ist keine Voraussetzung für die Meldepflicht.

Während die erste Meldepflicht an eine Schwachstelle im Produkt anknüpft, betrifft die zweite Meldepflicht Vorfälle, die die Sicherheit des Produkts beeinträchtigen – und damit auch solche, die auf einen Angriff auf die **Entwicklungs- oder Vertriebsprozesse des Herstellers** selbst zurückzuführen sind. Beispielsweise könnte ein Ransomware-Angriff auf die interne Entwicklungsinfrastruktur eines Herstellers dazu führen, dass böswilliger Code in eine Produktversion eingebettet wird, bevor diese an Kunden ausgeliefert wird.

Ab Kenntniserlangung

Maßgeblicher Auslöser der Meldepflicht ist in beiden Fällen der Zeitpunkt der **Kenntniserlangung.** Der CRA legt dabei nicht fest, auf welchem Weg oder durch welchen Kanal ein Hersteller Kenntnis erlangen muss – er verpflichtet ihn lediglich zur Meldung, sobald er Kenntnis erlangt hat.

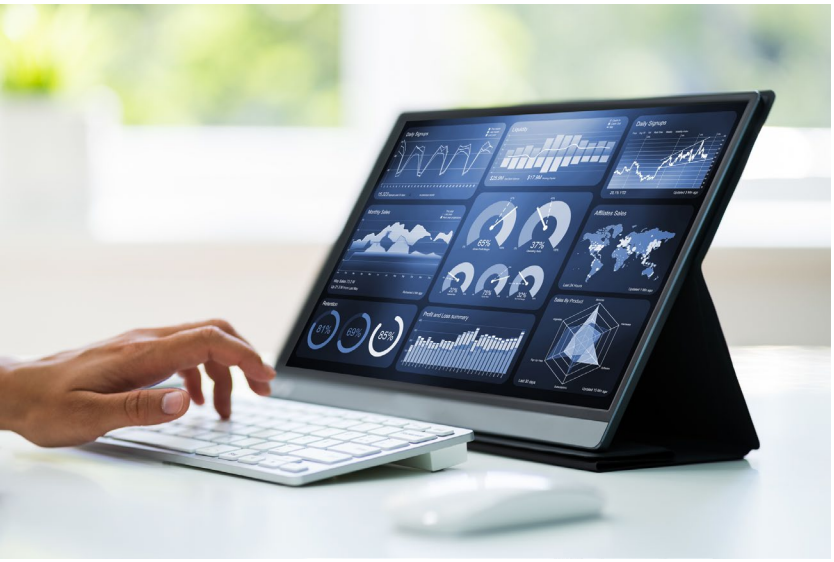
Einheitliche Meldeplattform

Die Meldung aktiv ausgenutzter Schwachstellen und schwerwiegender Sicherheitsvorfälle hat gleichzeitig an das als Koordinator benannte **CSIRT** (Computer Security Incident Response Team) und an die **ENISA** (Agentur der Europäischen Union für Cybersicherheit) zu erfolgen.

Hierfür richtet die ENISA eine **einheitliche Meldeplattform** ein, über die sämtliche Meldungen gemäß Artikel 14 CRA einzureichen sind. Diese Plattform stellt sicher, dass Meldungen technisch sicher übermittelt und gleichzeitig sowohl dem zuständigen nationalen CSIRT als auch der ENISA zugänglich gemacht werden.

Dreistufiges Melderegime

Artikel 14 CRA etabliert für beide Meldepflichttatbestände – aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle – ein **dreistufiges Melderegime**.



Stufe 1 – Frühwarnung

Unverzüglich, in jedem Fall aber innerhalb von **24 Stunden** nach Kenntniserlangung, ist eine Frühwarnung einzureichen.

An die inhaltliche Tiefe werden in dieser frühen Phase bewusst geringe Anforderungen gestellt. Erforderlich ist die Angabe der Mitgliedstaaten, in deren Hoheitsgebiet das Produkt bereitgestellt wurde. Bei schwerwiegenden Sicherheitsvorfällen ist darüber hinaus anzugeben, ob der Verdacht besteht, dass der Vorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist.

Die 24-Stunden-Frist beginnt nicht erst mit Abschluss einer vollständigen internen Untersuchung, sondern sobald der Hersteller mit einem vernünftigen Grad an Gewissheit feststellen kann, dass ein meldepflichtiges Ereignis vorliegt. Interne Eskalationswege müssen entsprechend kurz und klar definiert sein.

Stufe 2 – Folgemeldung

Unverzüglich, in jedem Fall aber innerhalb von **72 Stunden** nach Kenntniserlangung, ist – soweit die Informationen nicht bereits in der Frühwarnung enthalten waren – eine vertiefte Folgemeldung einzureichen.

Beide Meldespuren erfordern in dieser Stufe übereinstimmend allgemeine Informationen über das betroffene Produkt, Angaben zu bereits ergriffenen Korrektur- oder Risikominderungsmaßnahmen einschließlich solcher, die Nutzer selbst ergreifen können, sowie gegebenenfalls eine Sensitivitätseinstufung der gemeldeten Informationen.

Die Möglichkeit zur Sensitivitätseinstufung ermöglicht es dem Hersteller, auf eine vertrauliche Behandlung besonders sensibler Informationen hinzuwirken – etwa, wenn die Weitergabe technischer Details über eine noch nicht behobene Schwachstelle das Risiko weiterer Angriffe erhöhen würde.

Stufe 3 - Abschlussbericht

Bei aktiv ausgenutzten Schwachstellen ist der Abschlussbericht spätestens **14 Tage** nach Verfügbarkeit einer Korrektur- oder Risikominderungsmaßnahme einzureichen; bei schwerwiegenden Sicherheitsvorfällen innerhalb **eines Monats** nach Übermittlung der Folgemeldung.

Beide Meldespuren erfordern im Abschlussbericht übereinstimmend eine Beschreibung des Ereignisses einschließlich seines Schweregrads und seiner Auswirkungen sowie Angaben zu den getroffenen Korrektur- oder Abhilfemaßnahmen.

Pflicht zur Nutzerinformation

Parallel zu den behördlichen Meldepflichten sieht Artikel 14 Absatz 8 CRA eine **Benachrichtigungspflicht gegenüber den Nutzern** vor. Nach Kenntniserlangung hat der Hersteller betroffene und sofern erforderlich alle Nutzer unverzüglich über die Schwachstelle oder den Vorfall sowie über mögliche Risikominderungs- und Korrekturmaßnahmen zu informieren – gegebenenfalls in einem maschinenlesbaren Format.

Die Informationspflicht verpflichtet Hersteller nicht zur pauschalen öffentlichen Bekanntmachung jeder Schwachstelle. Die Nutzerkommunikation ist vielmehr risikobasiert und verhältnismäßig auszugestalten – insbesondere, wenn die Bekanntgabe technischer Details selbst ein Cybersicherheitsrisiko begründen könnte.

Informiert der Hersteller die Nutzer nicht rechtzeitig, können die als Koordinatoren benannten CSIRTs nach eigenem Ermessen aktiv in die Nutzerkommunikation eintreten. Dies birgt für Hersteller das erhebliche Risiko, die Kontrolle über die Kommunikation rund um einen Sicherheitsvorfall zu verlieren.

Bußgelder und weitere Konsequenzen

Der CRA sieht bei Verstößen gegen die Meldepflichten des Artikels 14 Geldbußen von bis zu **EUR 15 Mio.** oder von bis zu **2,5 % des gesamten weltweiten Jahresumsatzes** vor, je nachdem, welcher Betrag höher ist. Der Bußgeldrahmen orientiert sich damit an den aus dem Datenschutzrecht bekannten Sanktionssystemen. Die Geldbußen können zusätzlich zu anderen Korrektur- oder einschränkenden Maßnahmen der Marktüberwachungsbehörden verhängt werden.

Neben Geldbußen drohen **weitere Konsequenzen:** Marktüberwachungsbehörden können die Bereitstellung des Produkts untersagen, es vom Markt nehmen oder einen Rückruf anordnen. Hinzu kommen potenzielle Reputationsschäden durch die öffentliche Bekanntmachung von Verstößen sowie zivilrechtliche Haftungsrisiken, wenn die vorgeschriebene Nutzerinformation unterbleibt und Nutzer infolgedessen Schäden erleiden.

Pflichten der Händler

Die Meldepflichten des Artikels 14 richten sich zwar primär an Hersteller. **Der CRA verpflichtet jedoch auch Händler:** Sobald sie von einer Schwachstelle in einem Produkt mit digitalen Elementen Kenntnis erhalten, haben sie den Hersteller unverzüglich zu informieren.

Birgt das Produkt ein erhebliches Cybersicherheitsrisiko, haben Händler zudem **unverzüglich die Marktüberwachungsbehörden** der betroffenen Mitgliedstaaten zu unterrichten und dabei insbesondere Angaben zur Nichtkonformität und zu ergriffenen Korrekturmaßnahmen zu machen.

Handlungsempfehlungen

Die Meldepflichten des Artikels 14 CRA gelten ab dem 11. September 2026. Die verbleibende Zeit sollte genutzt werden, um die erforderlichen Strukturen aufzubauen. Folgende Maßnahmen sind empfehlenswert:

- **Bestandsaufnahme des Produktportfolios:** Hersteller sollten ermitteln, welche Produkte in den Anwendungsbereich des CRA fallen und welche Produkte bereits ab dem 11. September 2026 den Meldepflichten unterliegen.
- **Aufbau von Erkennungsfähigkeiten:** Hersteller müssen meldepflichtige Ereignisse erkennen können – etwa durch Überwachung einschlägiger Schwachstellendatenbanken.
- **Etablierung interner Eskalationsstrukturen:** Die kurzen Fristen erfordern vorab definierte Zuständigkeiten für die Bewertung meldepflichtiger Ereignisse, die Übermittlung über die ENISA-Meldeplattform und die parallele Nutzerkommunikation.
- **Anpassung von Lieferverträgen:** Lieferverträge sollten Informations-, Mitwirkungs- sowie Update-Pflichten der Zulieferer vorsehen, um die Meldepflicht auch bei Schwachstellen in Drittanbieterkomponenten erfüllen zu können.
- **Schulung und Vorbereitung:** Relevante Mitarbeiter aus Rechtsabteilung, IT-Sicherheit und Produktmanagement sollten frühzeitig geschult werden. Die Helpdesk-Angebote der nationalen CSIRTs sollten bereits vor Geltungsbeginn genutzt werden.

Ihre Ansprechpartner

Dr. Philipp Mels
Rechtsanwalt, Partner

T +49 211 60035-180
philipp.mels@orka.law

Felix Meurer
Rechtsanwalt, Salary Partner

T +49 30 509320-117
felix.meurer@orka.law