By PwC Deutschland | 11 September 2026

Sector Shorts: CRA-Meldepflichten - Warum Hersteller jetzt handeln sollten

Der Countdown läuft: Ab dem 11. September 2026 schreibt der Cyber Resilience Act (CRA) Herstellern vor, aktiv ausgenutzte Schwachstellen sowie schwerwiegende Sicherheitsvorfälle zu melden (Art. 14 CRA). Was das konkret bedeutet und warum sich Unternehmen schon jetzt damit auseinandersetzen sollten, zeigt der folgende Überblick

Wer ist betroffen?
Bevor wir uns den Meldepflichten im Detail widmen, lohnt sich ein Blick auf die grundsätzliche Reichweite des CRA. Denn diese ist denkbar weit gefasst.
Der CRA schafft einen einheitlichen Rechtsrahmen für die Cybersicherheit von „Produkten mit digitalen Elementen“ auf dem EU-Markt. Er reiht sich damit in den bekannten Rahmen der Marktüberwachungsverordnung ein und richtet sich – wie üblich – primär an Hersteller, aber auch an Händler, Einführer und Bevollmächtigte. Eine Besonderheit besteht darin, dass auch Verwalter quelloffener Software („Open Source Stewards“) erfasst werden, wenn auch mit reduzierten Pflichten.

Was zählt als „Produkt mit digitalen Elementen“?
Entscheidend für die Anwendbarkeit ist der bewusst weit und technologieneutral gefasste Produktbegriff. Erfasst ist grundsätzlich und einfach ausgedrückt jedes Software- oder Hardwareprodukt, das sich mit anderen Geräten oder Netzen verbinden kann. Damit fallen nicht nur physische Produkte mit digitalen Komponenten, sondern auch reine Software wie etwa Apps grundsätzlich unter den CRA. Aber auch Hard- und Softwarekombinationen sind erfasst: Ein Drucker mit zugehöriger Software bildet ebenso ein einheitliches Produkt wie eine App mit dem dazugehörigen Smarthome-Gerät oder Wearable.

Was genau ist zu melden?
Der CRA knüpft die Meldepflicht an zwei Auslöser. Zum einen sind aktiv ausgenutzte Schwachstellen eines Produkts mit digitalen Elementen zu melden. Gemeint ist damit eine Schwachstelle, für die es Belege gibt, dass ein Angreifer sie tatsächlich ausnutzt, ohne dass der Hersteller sie freigegeben hätte oder ohne dass es sich um einen Test handelt. Die bloße theoretische Existenz einer Sicherheitslücke reicht also nicht aus. Entscheidend ist die konkrete, laufende Ausnutzung. Dass die Schwachstelle in einer Drittkomponente vorliegt, entbindet nicht von der Meldepflicht, soweit die Ausnutzung im eigenen Produkt erfolgt.

Zum anderen sind schwerwiegende Sicherheitsvorfälle zu melden, die sich auf die Sicherheit des Produkts auswirken. Ein solcher Vorfall liegt insbesondere dann vor, wenn ein Ereignis die Fähigkeit des Produkts beeinträchtigt, die Verfügbarkeit, Integrität oder Vertraulichkeit sensibler Daten oder wichtiger Funktionen zu schützen, oder wenn es zur Einschleusung oder Ausführung von Schadcode im Produkt oder in den Systemen seiner Nutzer gekommen ist oder kommen kann.

In beiden Fällen greift ein gestaffeltes Verfahren mit engen Fristen. Hersteller müssen zunächst unverzüglich und in jedem Fall innerhalb von 24 Stunden eine Frühwarnung abgeben, anschließend innerhalb von 72 Stunden eine ausführlichere Meldung nachreichen und den Vorgang schließlich mit einer Abschlussmeldung innerhalb von 14 Tagen Vorhandensein ab Verfügbarkeit einer Korrekturmaßnahme (bei aktiv ausgenutzter Schwachstelle) bzw. einem Monat (bei schwerwiegendem Sicherheitsvorfall) abzuschließen. Wer diese Auslöser und die dahinterstehenden Fristen nicht kennt, kann im Ernstfall kaum rechtzeitig reagieren.

Wo ist zu melden?
Für die praktische Umsetzung der Meldepflichten hat die ENISA die „CRA Single Reporting Platform“ (SRP) online gestellt. Diese zentrale Anlaufstelle soll den Meldeprozess für Hersteller, Open Source Stewards und Bevollmächtigte vereinfachen. Wer sich mit den Anforderungen vertraut machen möchte,

findet auf der Webseite der ENISA weitere FAQs und Guidances, die erste Orientierung bieten. Die Meldung setzt grundsätzlich eine Registrierung und Validierung voraus. Die Registrierung soll nach Wunsch der ENISA aber erst erfolgen, soweit ein Vorfall initial zu melden ist. 20 „Freischuss-Meldungen“ vor Abschluss der Validierung sind laut aktuellen Informationen der ENISA möglich.

Wer ist noch zu informieren?

Neben der Meldung an Behörden verlangt der CRA auch eine Information der Nutzer. Hier unterscheidet das Gesetz zwischen „betroffenen Nutzern“ und „allen Nutzern“ eines Produkts mit digitalen Elementen, wobei Letztere nur „gegebenenfalls“ informiert werden müssen.

Der letzte Check: Kennen Sie Ihre Lieferkette?

Ab dem 11. September 2026 zählt jeder Tag. Meldepflichten lassen sich nur fristgerecht erfüllen, wenn Hersteller ihre eigenen Produkte und deren Bestandteile genau kennen. Wer jetzt noch keine belastbare Due-Diligence-Struktur für Drittkomponenten hat, gerät ins Risiko: Denn nur wer seine Lieferkette und Produktkomponenten transparent im Blick hat, kann im Ernstfall überhaupt erkennen, ob und wann eine Meldepflicht ausgelöst wird und die engen Fristen einhalten.

Fazit: Die Meldepflichten sind jetzt Realität

Mit dem 11. September 2026 endet die Vorbereitungszeit. Die Meldepflichten nach Art. 14 CRA sind ab diesem Zeitpunkt geltendes Recht und nicht mehr nur eine zukünftige Anforderung. Hersteller, die bislang keine funktionierenden Prozesse für Schwachstellen- und Vorfallsmeldungen implementiert haben, laufen ab sofort Gefahr, gesetzliche Fristen zu verpassen. Wer die eigene Lieferkette kennt, die SRP-Prozesse verstanden hat und klare interne Eskalationswege definiert hat, ist jetzt handlungsfähig.

Keywords

EU-Recht