Ein Leitfaden zum Verständnis der Cyberresilienz-Verordnung (EU Cyber Resilience Act (CRA))

Barracuda

Für Unternehmen, die in der EU Geschäfte tätigen, ist es unerlässlich, die Cyberresilienz-Verordnung der Europäischen Union zu verstehen. Hersteller von digitalen Produkten, die in der EU zum Verkauf angeboten werden, sowie die Importeure und Händler dieser Produkte unterliegen diesem Gesetz. Dieses E-Book bietet einige Highlights der Cyberresilienz-Verordnung für Hersteller, ist aber kein Ersatz und nicht als Rechtsberatung für Ihr Unternehmen gedacht.

Die Verordnung trat im Dezember 2024 in Kraft und gab den Unternehmen somit etwas Zeit, die Compliance zu erreichen. Hier sind einige wichtige Termine, die Sie wissen sollten:

- 11. September 2026 — Hersteller müssen schwerwiegende Cybersecurity-Vorfälle und aktiv ausgenutzte Schwachstellen melden.
- 11. Dezember 2027 — Alle neuen Produkte und alle „wesentlich veränderten“ bestehenden Produkte, die am oder nach diesem Datum in Verkehr gebracht werden, müssen den Bestimmungen der CRV entsprechen.

Das Gesetz soll einheitlichere Sicherheitsanforderungen für alle in der EU verkauften Produkte mit digitalen Elementen schaffen und Verbrauchern und Unternehmen, die diese Produkte kaufen, vor dem Kauf mehr Informationen über deren Sicherheit bereitstellen. Das Gesetz soll das beheben, was die EU als „unzureichendes Niveau“ der Cybersicherheit in vielen Produkten bezeichnet, darunter auch fehlende Sicherheitsupdates.

Der CRA ergänzt den Digital Operational Resilience Act (DORA) und die Network Information Security 2 Directive (NIS2):

- DORA konzentriert sich auf die Verbesserung der Cyber-Resilienz der Finanzbranche, und NIS2 gilt für eine breitere Gruppe von Unternehmen, die wesentliche Dienste in Schlüsselsektoren erbringen.
- Sowohl DORA als auch NIS2 legen Anforderungen an die Cybersecurity fest, einschließlich Maßnahmen zur Lieferkettensicherheit, um die Widerstandsfähigkeit der regulierten Unternehmen zu erhöhen, da ihre Angebote Auswirkungen auf andere Personen haben.
- Die CRV gilt auf Produktebene und bietet einen verbindlichen Rahmen für sichere Produkte mit digitalen Elementen. Wenn der Kunde solcher Produkte von DORA oder NIS2 reguliert wird, kann die Verwendung von CRV-konformer Hardware und Software diesen Unternehmen helfen, ihren Verpflichtungen nachzukommen.

NIS2 und DORA liegen außerhalb des Geltungsbereichs dieses E-Books. Weitere Details dazu siehe Was Sie über DORA wissen müssen: Ein Leitfaden zum Digital Operational Resilience Act und NIS2 verstehen: Ein Leitfaden zu den bevorstehenden europäischen Cybersecurity- Vorschriften.

Warum ist die CRV wichtig?

Die Cyberresilienz-Verordnung trifft auf alle Produkte zu, die „digitale Elemente“ enthalten. Das bedeutet, dass diese Verordnung sowohl Hardware als auch Software abdeckt, die mit einem Gerät oder Netzwerk verbunden ist, sowie integrierte Lösungen für die Datenfernverarbeitung (d. h. Cloud-Dienste) solcher Produkte. Die Europäische Kommission erklärt: „Die Verordnung gilt für alle Produkte, die direkt oder indirekt mit einem anderen Gerät oder Netzwerk verbunden sind, wobei bestimmte Ausnahmen gelten, wie z. B. bestimmte Open-Source-Software oder Dienstleistungsprodukte, die bereits durch bestehende Vorschriften abgedeckt sind, beispielsweise Medizinprodukte, die Luftfahrt und Autos.”[1] Nicht konforme Produkte dürfen in der EU nicht verkauft werden. Unternehmen, die dabei erwischt werden, müssen mit Geldstrafen rechnen. Genauso wie die Datenschutzgrundverordnung (DSGVO) den Umgang von Unternehmen mit personenbezogenen Daten grundlegend verändert hat, hat die Cyberresilienz-Verordnung das Potenzial, einen ähnlichen Effekt darauf zu haben, wie Hersteller ihre Produkte mit digitalen Elementen herstellen, verkaufen und unterstützen, die auf dem europäischen Markt angeboten werden.

Die Verordnung befasst sich mit einem wachsenden Problem moderner Technologieprodukte, die Nutzerdaten oft gar nicht oder nur unzureichend gesichert sammeln, verarbeiten, weitergeben und speichern und diese Daten dadurch gefährden. Mit zunehmendem Alter dieser Produkte können auch verfügbare Sicherheitslösungen veralten. Es gibt kaum Aufsicht darüber, wie, wann oder ob den Nutzern Sicherheits-Updates zur Verfügung gestellt werden. Die Verordnung möchte die Sicherheit von Produkten mit digitalen Elementen erhöhen und sicherstellen, dass sie während ihres gesamten Lebenszyklus sicher genutzt werden können. Das Gesetz sorgt auch für mehr Transparenz den Nutzern gegenüber, die ein besseres Verständnis für die Security von Produkten mit digitalen Elementen und deren mögliche Auswirkungen auf ihre Daten haben werden.

[1] Cyberresilienz-Verordnung | Gestaltung der digitalen Zukunft Europas

CRA-Verpflichtungen für Hersteller

Die CRV führt verbindliche Cybersicherheitsanforderungen für Hersteller ein, die die Planung, Konstruktion, Entwicklung, Produktion, Lieferung, Dokumentation und Wartung solcher Produkte regeln. Diese Verpflichtungen müssen in jeder Phase der Wertschöpfungskette erfüllt werden.

Gemäß der CRV können Produkte als „Standard“ (niedrigste Stufe), „Wichtig“ (mit mehr Verpflichtungen) — wobei letztere in zwei Unterkategorien unterteilt sind, „Wichtig Klasse I“ und „Wichtig Klasse II“ — oder „Kritisch“ (mit dem höchsten Risiko und damit den größten Verpflichtungen) klassifiziert werden.

Bei Standardartikeln sind die Hersteller verpflichtet, Waren und Dienstleistungen so zu entwickeln, herzustellen und zu testen, dass sie die in Anhang I der Verordnung festgelegten „wesentlichen Security-Anforderungen“ erfüllen (Compliance). Sie müssen auch die Bewertung dokumentieren und die technische Dokumentation den Marktüberwachungsbehörden zur Verfügung zu stellen. Auf dieser Ebene können sich Hersteller auf eine interne Konformitätsbewertung (Selbstbewertung) verlassen.

Im Allgemeinen dürften etwa 90 % der Hardware- und Softwareprodukte in diese Standardkategorie fallen, sodass die Hersteller Selbsttests durchführen und eine Konformitätserklärung erstellen können, bevor sie das CE-Zeichen auf konforme Produkte anbringen.

Bestimmte Produkte mit digitalen Elementen — wie Webbrowser, Firewalls und Betriebssysteme — fallen in die Kategorie „Wichtig“, andere sogar in die Kategorie „Kritisch“. Sie müssen ebenfalls die technischen Anforderungen des Anhangs I erfüllen, können jedoch einem strengeren Konformitätsbewertungsprozess unterliegen, einschließlich einer Bewertung oder Zertifizierung durch Dritte, bevor sie in der EU verkauft werden.

Zusätzlich zu den Verpflichtungen zum Zeitpunkt des Verkaufs verpflichtet die CRV die Hersteller auch zur Bereitstellung von Schwachstellenmanagement und Security-Patches, wie nachfolgend beschrieben.

Meldepflichten für Security

Die Meldepflicht aktiv ausgenutzter Security-Schwachstellen und schwerer Vorfälle nach der CRV tritt am 11. September 2026 in Kraft.

Die Meldepflichten sind streng. Die Hersteller müssen den Aufsichtsbehörden innerhalb von 24 Stunden nach Bekanntwerden der Angelegenheit eine „frühe Warnung“ übermitteln. Innerhalb von 72 Stunden nach Bekanntwerden einer ausgenutzten Schwachstelle müssen die Hersteller allgemeine Informationen über das betroffene Produkt, eine allgemeine Beschreibung der ausgenutzten Schwachstelle und alle Abhilfemaßnahmen, die der Hersteller ergriffen hat und die die Nutzer ergreifen können, bereitstellen sowie die Sensibilität des Problems angeben. Innerhalb von 14 Tagen nach Verfügbarkeit von Abhilfemaßnahmen hat der Hersteller weitere Informationspflichten im Sinne eines Abschlussberichts.

Zu den Meldepflichten gehört auch, betroffene Nutzer zu informieren und sie über Möglichkeiten zur Minderung des Risikos zu beraten.

Die Hersteller sollten sich mit diesen Meldepflichten vertraut machen und Prozesse entwickeln, um sie bis zum September zu erfüllen.

Verpflichtungen zum technischen Support

Cybersecurity-Support im Sinne der Bereitstellung von Sicherheitsupdates ist ebenfalls ein wichtiges Thema in der CRV und muss so geplant werden, dass er den gesamten Produktlebenszyklus abdeckt. Hersteller müssen die Supportdauer für Produkte mit digitalen Elementen im Voraus festlegen. Im Allgemeinen müssen Unternehmen, die Produkte mit digitalen Elementen in der EU auf den Markt bringen, diese mindestens fünf Jahre lang unterstützen, es sei denn, die erwartete Lebensdauer des Produkts beträgt weniger als fünf Jahre; in diesem Fall muss die Unterstützung für die erwartete Lebensdauer des Produkts gelten. Für Produkte, die im Allgemeinen eine längere Lebensdauer als fünf Jahre haben (Beispiele: Motherboards, Netzwerk-Router, Modems, Switches und Betriebssysteme), sollte der Supportzeitraum länger sein. Während des Supportzeitraums bereitgestellte Sicherheitsupdates müssen den Nutzern für den längeren Supportzeitraum oder 10 Jahre zur Verfügung stehen.

Wie wird die Compliance durchgesetzt?

Die Nichteinhaltung kann allgemeine Strafen und Geldbußen von bis zu 15 Millionen Euro oder 2,5 % des weltweiten Gesamtumsatzes nach sich ziehen. Die Aufsichtsbehörden haben die Handhabe, ein Unternehmen zum Rückruf nicht konformer Produkte zu zwingen.

Sechs Schritte zur Compliance für Hersteller

Im Folgenden finden Sie grundlegende Schritte für Hersteller, um mit dem Compliance-Prozess zu beginnen und für die CRV bereit zu sein, wenn diese vollständig in Kraft tritt. Die zahlreichen Anhänge der CRV enthalten detaillierte Angaben darüber, was bei jedem Schritt erwartet wird.

1. Klassifizieren Sie Produkte und führen Sie eine Cyberrisikobewertung durch. Die Produkte eines Unternehmens können in verschiedene Kategorien fallen. Daher ist es wichtig, jedes Produkt zu bewerten, um festzustellen, in welche Kategorie es fällt — „Standard“, „Wichtig“ oder „Kritisch“.

2. Bereiten Sie die technische Dokumentation vor. Prüfen Sie CRV Anhang I und die Anforderungen an die Lieferkette für alle Produkte und ermitteln Sie etwaige Lücken. Führen Sie für jedes Produkt eine Risikobewertung anhand der geltenden Kriterien und der ermittelten geeigneten Standards, gemeinsamen Spezifikationen oder Zertifizierungssysteme durch und dokumentieren Sie diese.

3. Bestimmen Sie den Ansatz zur Konformitätsbewertung für jedes Produkt. Beauftragen Sie gegebenenfalls einen Dritten mit dieser Aufgabe.

4. Erstellen Sie eine Konformitätserklärung gemäß Anhang V/VI und vervollständigen Sie die technische Dokumentation gemäß Anhang VII. Anschließend muss der Hersteller das CE-Zeichen auf einem konformen Produkt, dessen Verpackung oder Dokumentation anbringen. Die CE-Kennzeichnung bestätigt die Konformität von Produkten mit digitalen Elementen mit der CRV, sodass diese innerhalb der EU frei gehandelt werden können.

5. Bereiten Sie Nutzerinformationen/Anweisungen gemäß Anhang II vor und stellen Sie diese bereit. Die Dokumentation ist ein entscheidender Bestandteil der Compliance und ihres Ziels, Nutzern Transparenz zu bieten.

6. Überwachen und behandeln Sie Schwachstellen. Die Cyberresilienz-Verordnung verlangt von den Herstellern eine aktive und kontinuierliche Teilnahme während des Supportzeitraums, der die Bereitstellung von Cybersecuritymaßnahmen, die Überwachung von Schwachstellen sowie die Berichterstattung und Behebung von Problemen, wie z. B. Software-Updates zur Behebung von Sicherheitsproblemen, umfasst.

Barracuda arbeitet daran, seine Produktkategorien zu bestätigen und die nächsten Schritte anzugehen. Wir werden Informationen über das Trust Center bereitstellen, sobald verfügbar.

SCHRITT 1
Produkte klassifizieren und Cyber-Risikobewertungen durchführen

SCHRITT 2
Technische Dokumentation erstellen

SCHRITT 3
Ansatz für die Konformitätsbewertung festlegen

SCHRITT 4
CE-Marketing anwenden und Konformitätserklärung entwerfen

SCHRITT 5
Nutzeranweisungen vorbereiten und bereitstellen

SCHRITT 6
Schwachstellen überwachen und beheben

Wichtige Klasse I und Wichtige Klasse II

Produkte der Kategorie „Wichtig Klasse I“ stellen ein geringeres Cybersicherheitsrisiko dar als Produkte der Kategorie „Wichtig Klasse II“. Hersteller können sich dafür entscheiden, die Konformität selbst zu erklären, wenn sie bestimmte qualifizierte EU-Standards/gemeinsame Spezifikationen/ Zertifizierungssysteme einhalten, sofern diese verfügbar und auf das Produkt anwendbar sind. Andernfalls kann eine Überprüfung durch einen Dritten erforderlich sein.

Bei wichtigen Produkten der Klasse II wird ein höheres Cybersecurity-Risiko angenommen, weshalb eine Zertifizierung durch eine autorisierte Drittpartei erforderlich ist.

Die Cyberresilienz-Verordnung, DORA und NIS2 bilden zusammen eine komplexe Reihe von Cybersicherheitsvorschriften für Unternehmen, die in der EU Geschäfte tätigen. Ihr Unternehmen unterliegt möglicherweise mehr als einer dieser Vorschriften. Das Trust Center von Barracuda enthält mehrere Ressourcen, die Kunden dabei helfen, DORA zu verstehen, darunter unser E-Book Was Sie über DORA wissen müssen: Ein Leitfaden zum Digital Operational Resilience Act und unser E-Book NIS2 verstehen: Ein Leitfaden zu den bevorstehenden europäischen Cybersecurity-Vorschriften, um Unternehmen bei ihren Compliance-Verpflichtungen zu unterstützen.

Über Barracuda

Barracuda ist ein weltweit führendes Cybersecurity-Unternehmen, das Unternehmen jeder Größe umfassenden Schutz vor komplexen Bedrohungen bietet. Unsere KI-gestützte Plattform BarracudaONE schützt E-Mails, Daten, Anwendungen und Netzwerke mit innovativen Lösungen, einem Managed XDR-Service sowie einem zentralen Dashboard. Das sorgt für maximalen Schutz und stärkt die Cyber-Resilienz. Von Hunderttausenden von IT-Experten und Managed Service Providern weltweit als vertrauenswürdig angesehen, bietet Barracuda leistungsstarke Abwehrmaßnahmen, die einfach zu erwerben, bereitzustellen und zu verwenden sind. Weitere Informationen erhalten Sie auf de.barracuda.com.

Barracuda