



Der Cyber Resilience Act (CRA) ist in Kraft.

CRA: Die Anforderungen sind nun verbindlich. Welche Pflichten kommen als Hersteller auf Sie zu?

Mit dem Cyber Resilience Act (CRA) soll die Cybersicherheit vernetzbarer Produkte auf ein EU- und produktübergreifend hohes, einheitliches Niveau gehoben und die Transparenz von Sicherheitseigenschaften verbessert werden. Die Regulierung ist sektorübergreifend und umfasst alle Bereiche der Cybersecurity und alle Produkte, die eine Datenverbindung zu einem anderen Produkt oder einem Netzwerk aufbauen können.

Hersteller müssen grundsätzlich für jedes Produkt „mit digitalen Elementen“ ein Cybersecurity Risk Assessment durchführen und „das Ergebnis dieser Bewertung in der Planungs-, Konzeptions-, Entwicklungs-, Herstellungs-, Liefer- und Wartungsphase des Produkts“ berücksichtigen (Art. 10 Abs. 2). Die Anforderungen gelten also für den gesamten Lebenszyklus. Darüber hinaus müssen Hersteller ein Risikomanagement und effektives Schwachstellenmanagement implementieren. Für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle gelten Meldepflichten mit engen zeitlichen Fristen. Zudem müssen sie Updates und Patches zur Behebung der Schwachstellen bereitstellen. (Anhang I, Teil I Abs. 2c).

Ab wann gilt der Cyber Resilience Act?

Ende 2023 einigten sich die Europäische Kommission, das Europäische Parlament und der Rat der Europäischen Union auf den endgültigen Text des CRA. Am 20. November 2024 wurde er im EU-Amtsblatt veröffentlicht und trat am 10. Dezember 2024 in Kraft. Um Unternehmen Zeit für die Umstellung zu geben, müssen die Anforderungen aber nicht mit sofortiger Wirkung umgesetzt werden. Ab dem 11. Juni 2026 werden die Konformitätsbewertungsstellen ermächtigt, die CRA-Konformität zu bewerten. Ab dem 11. September 2026 unterliegen Hersteller der Meldepflicht für Schwachstellen und Vorfälle. Ab dem 11. November 2027 gelten alle Anforderungen in vollem Umfang.



Normen & Standards

Wir unterstützen bei der Erfüllung der CRA-Konformität auf Basis dieser Normen / Standards:

- ISA/IEC 62443 – Industrie
- ETSI EN 303 645 – Consumer IoT
- EN ISO/IEC 27xxx – IT-Security
- IEC 63452 – Railway
- etc.





Managing CRA: NewTec-Leistungen zur Erfüllung der gesetzlichen Anforderungen

NewTec unterstützt Hersteller bei der CRA-konformen Entwicklung von Produkten mit digitalen Elementen – beispielsweise bei einer dem Cyber Resilience Act entsprechenden Gefahren- und Risikoanalyse, der Integration von Sicherheitsmaßnahmen oder der Implementierung sicherer Updateprozesse sowie einem umfassenden Security-Testing. Unsere Experten führen mit Ihnen eine Standortbestimmung durch, geben Hilfe bei der Klassifizierung und unterstützen bei der Einführung notwendiger Prozesse sowie dem sicheren Betrieb.

<p>Befähigung Ihrer Organisation:</p> <ul style="list-style-type: none"> • CRA GAP-Analyse: Reifegradbestimmung der Entwicklungs- und Begleitprozesse • Einführung von CRA-konformen Prozessen • Dokumentation gemäß CRA • Workshops und Trainings zum Aufbau von Security-Awareness und Know-how 	<p>CRA-konforme Produktentwicklung</p> <ul style="list-style-type: none"> • Produktklassifizierung • Erstellung Cyber Security Management Plan • Entwicklung und Dokumentation gemäß CRA • Risikoanalysen während des gesamten Produktlebenszyklus (TARA, IRA, DRA) • Entwicklung sicherer Update-Strategien • Beratung und Unterstützung bei der Konformitätsprüfung zum CRA 	<p>Sicherer Betrieb/ Vorfallsmanagement</p> <ul style="list-style-type: none"> • Automatisiertes Schwachstellenmonitoring • Schwachstellenmanagement • Update-Management • Unterstützung in Form eines kundenindividuellen Product Security Incident Response Team (PSIRT): • Bereitstellung einer Public-Key-Infrastruktur (PKI)
--	---	--