Pflicht zur Sicherheit über den gesamten Produktlebenszyklus

Mit der Verabschiedung des Cyber Resilience Act (CRA) im Oktober 2024 hat die Europäische Union einen Meilenstein für die Cybersicherheit von Produkten mit digitalen Elementen gesetzt. Spätestens ab dem 11. Dezember 2027 dürfen nur noch Produkte mit gültiger CE-Kennzeichnung auf den Markt gebracht werden, die den CRA-Anforderungen entsprechen.

Schon ab 11. September 2026 greifen Meldepflichten für schwerwiegende Vorfälle und aktiv ausgenutzte Schwachstellen. Für Hersteller von Embedded-Systemen, Medizintechnik und Industrieelektronik bedeutet dies: Sicherheitskonzepte müssen tief in Entwicklungs- und Organisationsprozesse integriert werden. Gleichzeitig entstehen neue Anforderungen an Lieferketten, an die Updatefähigkeit und an die Nachweisführung gegenüber Behörden.

Ginzinger electronic systems GmbH
www.ginzinger.com

Hintergrund und Zielsetzung

Die digitale Vernetzung wächst rasant - sei es in industriellen Steuerungen, medizinischen Geräten, IoT-Komponenten oder alltäglichen Konsumprodukten. Damit steigen auch die Angriffsflächen. Schwachstellen entstehen nicht nur durch mangelhafte Entwicklung, sondern durch zunehmende technische Komplexität, intensivere Analysen sowie die Professionalität von Angreifenden.

Der CRA soll sicherstellen, dass Sicherheitsrisiken frühzeitig erkannt und Produkte auch im Feld kontinuierlich geschützt werden. Damit etabliert die EU erstmals ein übergreifendes, produktgruppenunabhängiges Regelwerk, das für Hersteller, Importeure und Händler gleichermaßen gilt. Betroffen sind sämtliche Hard- und Softwareprodukte mit Datenverarbeitungs- oder Kommunikationsschnittstellen.

Seltene Ausnahmen

Ausnahmen bestehen nur für bereits streng regulierte Bereiche wie Luftfahrt, Verteidigung oder In-vitro-Diagnostik. Besonders bemerkenswert ist, dass mit dem CRA erstmals auch kleine und mittelständische Unternehmen systematisch verpflichtet werden, professionelle Security-Prozesse einzuführen.

Während Großkonzerne bereits etablierte Abteilungen für Cybersecurity betreiben, bedeutet dies für viele KMU einen erheblichen organisatorischen und finanziellen Aufwand.

Zentrale Anforderungen des CRA

Hersteller müssen künftig eine Vielzahl technischer und organisatorischer Maßnahmen nachweisen. Im Mittelpunkt stehen:

- **Risikobasierte Sicherheitskonzepte**

  Sicherheit ist über den gesamten Produktlebenszyklus hinweg zu berücksichtigen **- von der Architektur über die Entwicklung bis hin zu Updates im Feld.**

  Konkrete Maßnahmen gibt der CRA nicht vor, stattdessen verlangt er nachvollziehbare, dokumentierte Risikoanalysen.

- **Software Bill of Materials (SBoM):**

  Eine vollständige, maschinenlesbare Auflistung aller Software-Komponenten (z. B. SPDX, CycloneDX) wird Pflicht. Sie ermöglicht Transparenz über verwendete Bibliotheken und erleichtert das Schwachstellenmanagement.

- **Schwachstellenmanagement:**

  Hersteller müssen Prozesse zur Entdeckung, Bewertung und Behebung von Schwachstellen implementieren. Dazu gehören Meldewege, klare Verantwortlichkeiten und ein strukturierter Umgang mit Sicherheitslücken.

- **Sicherheitsupdates:**

  Updates sind kostenfrei, sicher (signiert, verschlüsselt) und über definierte Zeiträume bereitzustellen - in der Regel mindestens fünf Jahre. Produkte sollen standardmäßig automatische Sicherheitsupdates unterstützen.

- **Meldepflichten:**

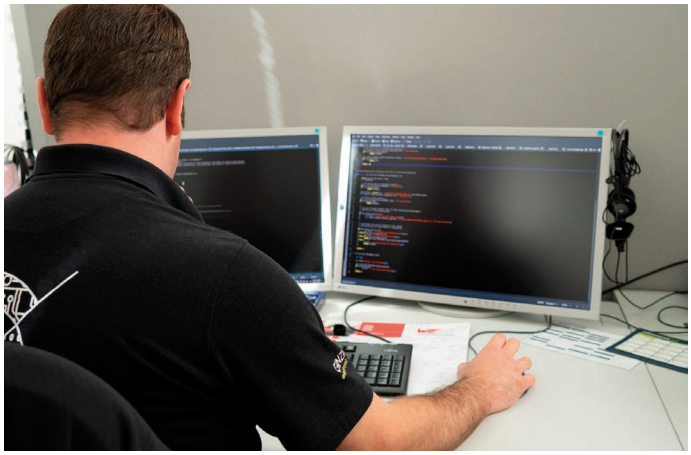
  Schwerwiegende Vorfälle und aktiv ausgenutzte Schwachstellen müssen binnen 24 bis 72 Stunden an nationale CERTs und an die EU-Agentur ENISA gemeldet werden.

- **Dokumentation:**

  Neben technischen Beschreibungen sind Bedrohungsanalysen, Sicherheitskonzepte und Nachweise über den Unterstützungszeitraum vorzulegen.

Klassifizierung und Sanktionen

Der CRA unterscheidet Produkte nach Relevanz: von „nicht klassifiziert“ bis „kritisch“. Je nach Einstufung reichen die Nachweise von Selbstdeklarationen bis hin zu zwingenden, externen Prüfungen oder Zertifizierungen. Bei Verstößen drohen Bußgelder bis zu 15 Mio. Euro oder 2,5 % des weltweiten Jahresumsatzes - je nachdem, welcher Wert höher ist.



Marktaufsichtsbehörden können zudem Produkte vom Markt nehmen oder Rückrufe anordnen. Dies bedeutet, dass nicht nur technische, sondern auch wirtschaftliche Risiken für Unternehmen dramatisch steigen. Für Zulieferer entsteht dadurch ein zusätzlicher Druck, ihre Kunden rechtzeitig mit validierten Komponenten zu beliefern.

Relevanz für Embedded-und Medizingeräte

Besonders Embedded-Systeme stehen im Fokus, da sie häufig über lange Lebenszyklen, begrenzte Ressourcen und komplexe Lieferketten verfügen. Hier erfordert der CRA eine besonders sorgfältige Umsetzung.

Security by Design ist gesetzlich vorgeschrieben. Schnittstellen wie USB oder Ethernet müssen dokumentiert, abgesichert und bei Bedarf deaktivierbar sein. langfristige Updatefähigkeit ist auch für Geräte ohne permanente Netzwerkanbindung sicherzustellen, z. B. über USB oder Wartungsschnittstellen.

Für Medizintechnikhersteller ergibt sich eine Doppeltregulierung: Neben der MDR (Medical Device Regulation) müssen auch die (RA-Vorgaben umgesetzt werden. Da Patientensicherheit und Datenschutz direkt betroffen sind, gilt hier ein besonders hohes Schutzniveau. Unternehmen müssen nachweisen, dass Sicherheitsupdates die Funktionalität der Geräte nicht beeinträchtigen - ein erheblicher Mehraufwand in Validierung und Dokumentation.

Erste Schritte für Hersteller

Die Umsetzung des CRA erfordert strategische Vorbereitung. Folgende Maßnahmen gelten als praxisbewährter Einstieg:

1. Threat & Risk Assessment (TRA):

Systematische Bedrohungsanalysen, ähnlich wie in Safety-Prozessen, bilden die Grundlage.

2. SBoM-Integration in die Build-Pipeline:

Automatisierte Erzeugung und Pflege der Software-Stückliste spart Aufwand und schafft Transparenz.

3. Strukturiertes Schwachstellenmanagement:

Definierte Prozesse für Eingang, Bewertung und Meldung von Sicherheitslücken.

4. Update-Strategie:

Planung robuster und sicherer Updatewege, auch für Offline-Geräte.

5. Schulung & Bewusstsein:

Interdisziplinäre Teams - von Entwicklung über Support bis zum Management - müssen in den CRA-Anforderungen geschult werden.

Ergänzend sollten Hersteller auch ihre Verträge mit Zulieferer überprüfen: Security-Kriterien werden künftig fester Bestandteil von Lieferbedingungen sein. Ebenso ist es ratsam, frühzeitig den Dialog mit Benannten Stellen und Behörden zu suchen, um Interpretationsspielräume abzuklären.

Praxisbeispiel: IoT-Adapter ohne Cloud-Anbindung

Ein Beispiel aus der Praxis: Ein Smart-Meter-Adapter kommuniziert lokal mit dem Heimnetzwerk, bewusst ohne Cloud-Anbindung. Dadurch werden Angriffsflächen reduziert. Dennoch sind Aspekte wie Authentifizierung, Schnittstellensicherheit und Verschlüsselung zu beachten.

Die Bedrohungsanalyse deckt hier Szenarien wie manipulierte Firmware, Datenabgriffe oder ungeschützte Ports auf. Das Ergebnis ist ein klarer Maßnahmenplan, der bereits in der frühen Entwicklungsphase umgesetzt werden kann. Dieses Beispiel verdeutlicht, dass der CRA nicht nur als bürokratische Last zu verstehen ist, sondern Innovationspotenzial freisetzen kann: Produkte mit hoher Sicherheit und Transparenz verschaffen einen Marktvorteil.

Unterstützung durch Standards und Partner

Aktuell existieren noch keine harmonisierten Normen zum CRA. Als Wegweiser gelten jedoch Standards wie die IEC 62443 (sichere Entwicklungsprozesse, technische Sicherheitsanforderungen). Sie bieten eine solide Grundlage, auch wenn sie keine formale Rechtssicherheit garantieren. ISO-Normen zu Software-Qualität und Informationssicherheit (z. B. ISO 27001, ISO 9001) ergänzen das Gerüst.

Unternehmen unterstützen Hersteller mit Plattformlösungen (z. B. Embedded Linux GELin mit integriertem SBoM-Management), robusten Updateprozessen und ISO-zertifizierten Entwicklungsabläufen. In Zusammenarbeit mit Security-Experten lassen sich so tragfähige Strategien entwickeln - sowohl für Medizintechnik als auch für industrielle Anwendungen.

Der Cyber Resilience Act verändert die Spielregeln

Cybersicherheit ist nicht länger optional, sondern wird zur gesetzlichen Voraussetzung für Marktzugang in Europa. Für Hersteller bedeutet dies, Entwicklungsprozesse, Supportstrategien und Dokumentationen konsequent neu zu denken. Wer jetzt mit Risikoanalysen, Updatekonzepten und SBoM-Integration beginnt, sichert nicht nur die rechtzeitige Konformität bis 2027, sondern verschafft sich auch einen Wettbewerbsvorteil: Sichere Produkte sind künftig ein zentrales Verkaufsargument - in der Industrie ebenso wie in der Medizintechnik. ◄

Downloadtipp:

Das gemeinsame CRA-Whitepaper „Sind Sie bereit für den CRA“ von Ginzinger electronic systems und Limes Security (www.limessecurity.com), langjähriger Partner von Ginzinger in Sachen Security:

www.ginzinger.com/CRAWhitepaper

Das Whitepaper kann außerdem als Print-Version angefordert werden!