Checkliste

Cyber Resilience Act: Der Praxisleitfaden für Hersteller

LINOVA

Wie können Unternehmen sinnvoll vorgehen?

Der Cyber Resilience Act (CRA) stellt unter anderem Hersteller vor neue Anforderungen an Cybersicherheit, Risikomanagement, Dokumentation und Meldeprozesse. Betroffen sind vor allem Unternehmen, die Produkte mit digitalen Elementen, Software oder digitale Komponenten auf den EU-Markt bringen.

Diese Checkliste hilft Herstellern dabei, die wichtigsten Handlungsfelder systematisch zu prüfen. Sie ersetzt keine rechtliche Bewertung, schafft aber eine erste Orientierung: Welche Produkte sind betroffen? Welche Sicherheitsanforderungen müssen umgesetzt werden? Welche Nachweise, Prozesse und Verantwortlichkeiten müssen vorbereitet werden?

Wenn Sie bei der Einordnung, Planung oder technischen Umsetzung Unterstützung benötigen, sprechen Sie uns gerne an. Wir unterstützen Sie dabei, die Anforderungen des CRA strukturiert zu prüfen und in konkrete Maßnahmen zu übersetzen.

Checkliste für Hersteller zur Umsetzung des CRA

1. Relevanz & Betroffenheit klären

- ○ Produkte mit digitalen Elementen sind auf dem EU-Markt im Umlauf
- ○ Produkte fallen nicht unter ausgenommene, anderweitig regulierte Produktgruppen
- ○ Inkrafttreten der geltenden Fristen ist bekannt (Meldepflichten ab 11.09.2026; vollständige Anwendung der meisten Herstellerpflichten ab 11.12.2027)

---

2. Produkt- & Risikoeinordnung vornehmen

- ○ Betroffene Produkte sind vollständig identifiziert
- ○ Produkte wurden einer CRA-Produktkategorie zugeordnet
- ○ „Kritische" bzw. „wichtige" Produkte sind bekannt
- ○ Konformitätsbewertungsverfahren ist festgelegt (Selbstbewertung/ benannte Stelle)

---

3. Governance & Verantwortung festlegen

- ○ Verantwortung für CRA-Umsetzung ist benannt
- ○ Produkt-, IT-, Security-, Rechts- und Compliance-Funktionen sind eingebunden
- ○ CRA ist in bestehende Management- und Compliance-Strukturen integriert

---

4. Security-Grundlagen sicherstellen

- ○ Cyber-Risiken der Produkte sind bewertet
- ○ „Security by Design" und „Security by Default" sind verbindliche Entwicklungsgrundsätze
- ○ Schwachstellen- und Patch-Management ist etabliert
- ○ Sicherer Update-Mechanismus ist vorhanden
- ○ Grundlegende Anforderungen an Cybersicherheit beachten (siehe auch CRA Anhang I)

5. Melde- & Reaktionsfähigkeit gewährleisten

- ○ Prozesse zur Meldung aktiv ausgenutzter Schwachstellen und schwerwiegender Sicherheitsvorfälle sind eingerichtet (Frühwarnung innerhalb von 24 Stunden, Meldung innerhalb von 72 Stunden und fristgerechter Abschlussbericht)
- ○ Verantwortlichkeiten und Eskalationswege sind definiert
- ○ Melde- und Reaktionsprozesse sind auch für bereits in Verkehr gebrachte Produkte definiert

---

6. Support & Lebenszyklus definieren

- ○ Support- und Update-Zeiträume sind festgelegt (Supportdauer ist angemessen zur Produktlebensdauer, mind. 5 Jahre)
- ○ Kunden werden vor bzw. beim Kauf transparent über das Enddatum des Unterstützungszeitraums sowie die Sicherheits- und Nutzungsinformationen informiert

---

7. Dokumentation & Nachweise vorbereiten

- ○ Technische Dokumentation liegt vollständig vor (Produktbeschreibung, Architektur-/Entwicklungsinformationen, Risikobewertung, Vulnerability-Handling-Prozesse, SBOM, Prüf-/Testnachweise und die angewandten Konformitätsnachweise; siehe CRA Anhang VII)
- ○ Software Bill of Materials (SBOM) ist erstellt und gepflegt
- ○ EU-Konformitätserklärung kann ausgestellt werden
- ○ CE-Kennzeichnung ist vorbereitet

---

8. Lieferkette & Drittparteien absichern

- ○ Sicherheitsanforderungen an Lieferanten sind definiert
- ○ Abhängigkeiten und integrierte Drittkomponenten sind erfasst, Verantwortlichkeiten für deren Aktualität und Sicherheit sind festgelegt
- ○ Schwachstelleninformationen und Sicherheitsupdates entlang der Lieferkette sind geregelt

---

9. Risiken & Sanktionen prüfen

- ○ Mögliche Bußgelder und Haftungsrisiken sind bewertet
- ○ Risiken sind im Management-Reporting berücksichtigt
- ○ Maßnahmen werden nach Cybersicherheitsrisiko, Umsetzungsfrist, Compliance-Relevanz und Sanktionsrisiko priorisiert

Wenn die Zeit oder das Wissen fehlt, sind wir gerne der Partner an Ihrer Seite!

Wir unterstützen Unternehmen dabei, Systeme, Geräte und Datenquellen zu vernetzen und in eine durchgängige, datenbasierte Entscheidungs- und Steuerungsbasis zu überführen. Dabei realisieren wir Lösungen zur Steuerung, Inbetriebnahme und Überwachung bislang autark arbeitender Geräte über mobile Endgeräte sowie zur Fernwartung und Zustandsüberwachung von Anlagen. Ein zentraler Fokus liegt auf der Erfassung, zentralen (cloudbasierten) Speicherung und Analyse von nutzungs-, system- und nutzerspezifischen Daten.

Die Anbindung und Integration heterogener Systemlandschaften – einschließlich proprietärer Schnittstellen, Protokolle und gewachsener Infrastrukturen – ist dabei ein wesentlicher Bestandteil unserer Arbeit. Auf dieser Basis schaffen wir datengetriebene Anwendungen in den Bereichen Business Intelligence (BI), Monitoring und Visualisierung und entwickeln individuelle Dashboards für operative und strategische Entscheidungsprozesse. Ergänzend setzen wir gezielt Analytics- und KI-Methoden ein, um Daten zu analysieren, Zusammenhänge zu verstehen und Entwicklungen vorherzusagen. Gemeinsam mit unseren Kunden erarbeiten wir pragmatische Integrations- oder Migrationsstrategien und ermöglichen so die strukturierte Auswertung großer Datenmengen aus Sensoren, Anlagen und Anwendungen.

Jetzt 30 Minuten kostenfreies Orientierungsgespräch buchen!

Sollten Sie Fragen haben oder Unterstützung bei der Umsetzung benötigen, helfe ich Ihnen gerne weiter.

Termin vereinbaren

Sandra von König
Senior Sales Manager

Tel.: +49 89 4524668-21
Mobil: +49 176 45552391
Mail: sandra.von.koenig@linova.de

Ich freue mich auf unser Gespräch!