secuvera:
Cybersicherheit. Nachhaltig.

Erfahrungen und Umsetzungsvorschläge für den Cyber Resilience Act (CRA)

Luise Werner, secuvera GmbH

Agenda

secuvera:
Cybersicherheit. Nachhaltig.

1. Der Cyber Resilience Act
2. Projekterfahrungen
3. Die CRA-Toolbox
4. Fazit

secuvera:
Cybersicherheit. Nachhaltig.

Der CRA

Wann?

secuvera:
Cybersicherheit. Nachhaltig.

- seit 11. Dezember 2024 in Kraft
  - Meldepflicht von Schwachstellen: 11. September 2026
  - Konformitätsbewertung ab Juni 2026 möglich
  - Einhaltung in allen Produkten: 11. Dezember 2027
  - ab dann Pflicht für CE-Kennzeichen!
- aktuell fehlen noch: harmonisierte Standards
  - in Arbeit

Warum?

secuvera:
Cybersicherheit. Nachhaltig.

- Fokus: Produkte mit digitalen Elementen
  - alle Hardware- und Software-Produkte, zu deren Verwendung eine direkte oder indirekte Datenverbindung mit einem Gerät oder Netz notwendig ist
- Gilt nicht für anderweitig regulierte Produkte:
  - Medizinprodukte, KFZ, Zivilluftfahrt und Flugsicherheit, Verteidigung
  - reine Cloudprodukte

Wer?

secuvera:
Cybersicherheit. Nachhaltig.

- CRA Produktklassen
  - Nicht klassifizierte Produkte
  - Wichtige Produkte Klasse 1

  Keine externe Prüfung notwendig
  - Wichtige Produkte Klasse 2
  - Kritische Produkte

  Externe Prüfung notwendig

Was?

secuvera:
Cybersicherheit. Nachhaltig.

Bis zu 15 Millionen Euro

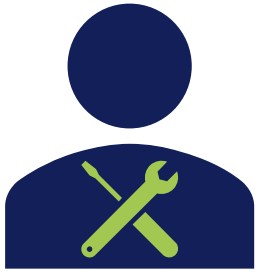
Bis zu 2,5 % des globalen jährlichen Umsatzes

Höchststrafen bei Verstoß gegen:

- Artikel 13 - Pflichten der Hersteller
- Artikel 14 - Meldepflichten der Hersteller

Rollen im CRA

secuvera:
Cybersicherheit. Nachhaltig.



Hersteller

Produziert in EU-Inland

Verantwortlich für Konformität des eigenen Produkts

Händler

Produkte aus EU-Inland

Verantwortlich für Prüfung auf CE-Kennzeichen und Pflichtinformationen

Einführer

Produkte aus EU-Ausland

Verantwortlich für Konformität des importierten Produkt

Pflichten als Hersteller

secuvera:
Cybersicherheit. Nachhaltig.

- Erfüllung der grundlegenden Anforderungen
- Risikobewertung
- Festlegung eines verbindlichen Unterstützungszeitraums
- Anfertigen und Aufbewahren einer technischen Dokumentation
- Kontrollierter Einsatz von Drittkomponenten ohne Beeinträchtigung de heit
- Meldung von Schwachstellen, die in Drittkomponenten festgestellt
- Dokumentation aller relevanten Cybersicherheitsaspekte wie Schw nd Vo
- Behandlung von Schwachstellen während der erwarteten Leben s fes stütz
- Bereithalten von Sicherheitsaktualisierungen
- Information der Nutzer über die Risiken der Verwendung von n
- Durchführung und Vorhalten der Dokumentation eines Konform s
- Anbringen des CE-Kennzeichens
- Qualitätssicherung
- Berücksichtigen und Nachverfolgen von Änderungen an der EU- isier
- Anbringen einer Typen-, Chargen- oder Seriennummer oder eines
- Angabe von Informationen zum Hersteller (Name, Postanschrift, E- site, ze i Schwachstellen, Ende des Unterstützungszeitraums) auf dem Produkt selbst, der Verpackung oder beigefügten Unterlagen
- Bereitstellen einer leicht zu ermittelnden Meldestelle für Schwachstellen
- Anfertigen und Bereitstellen der Informationen und Anleitungen für den Nutze
- Anzeige einer Meldung zum Ende des Unterstützungszeitraums sofern technisch mögl
- Beifügen einer Kopie der EU-Konformitätserklärung oder der vereinfachten EU-Konformitätserklärung mit Verweis auf die vollständige Erklärung
- Rückruf oder Korrektur von Produkten bei Bekanntwerden der Nicht-Konformität
- Auf Anfrage Übermittlung aller Informationen und Unterlagen zum Nachweis der Konformität an die zuständigen Behörden
- Information der Marktüberwachungsbehörde und soweit möglich der Nutzer bei Betriebseinstellung

Pflichten als Hersteller

secuvera:
Cybersicherheit. Nachhaltig.

Produktanforderungen

Anhang I – Teil 1

Technische Dokumentation

Anhang VII

Anforderungen an das Schwachstellenmanagement

Anhang I – Teil 2

Produktbegleitende Dokumente für den Nutzer

Anhang II

Themenblöcke

secuvera:
Cybersicherheit. Nachhaltig.

secuvera:
Cybersicherheit. Nachhaltig.

Projekterfahrungen

Projekterfahrungen

secuvera:
Cybersicherheit. Nachhaltig.

- Konzernprojekte
  - CISO
  - Security Know-How in Produktteams (manchmal)
  - Zentrale Strukturen, lokale Produktteams
  - Lieferkette (3rd-Party-Management)

Projekterfahrungen

secuvera:
Cybersicherheit. Nachhaltig.

- KMU-Projekte
  - Bin ich überhaupt betroffen?
  - Wie kann ich den CRA mit möglichst wenig Aufwand umsetzen?
  - Produkt-Triage: Neu, Abkündigung, Modernisierung

Projekterfahrungen

secuvera:
Cybersicherheit. Nachhaltig.

- CE-Kennzeichnung
  - QM-Abteilung
  - Technische Dokumentation
    - zentrale Ablage?
  - „CE-Verantwortlicher für Cybersecurity“
  - Module H (Qualitätssicherungsprozess)

Projekterfahrungen

secuvera:
Cybersicherheit. Nachhaltig.

- Herausforderungen
  - Knappe Ressourcen
  - Standard oder Freestyle
  - Prozesse aufsetzen vs. ad-hoc Vorgehen
  - Skalierung von Methoden
  - Fehlender Wille
  - Fehlendes Wissen der Lieferkette

Häufige Fragen

secuvera:
Cybersicherheit. Nachhaltig.

- Wo fange ich mit der Umsetzung an?
- Wie erstelle ich eine **Risikoanalyse**?
- In welche **Kategorie** fällt mein Produkt?
- Wie gehe ich mit **3rd-Party-Komponenten** um?
- Wie kann ich meine eigene **Konformität** prüfen?

secuvera:
Cybersicherheit. Nachhaltig.

Die CRA-Toolbox

Was steckt in der Toolbox?

secuvera:
Cybersicherheit. Nachhaltig.

Anfang	CRA-Einführung
Risikoanalyse	Vorlage zur Risikoanalyse
Produktkategorie	Vorlage zur Produktbewertung
3rd-Party-Komponenten	Checkliste zur Bewertung von Drittkomponenten
Konformitätsprüfung	Vorlagen zur Technischen Dokumentation und zur Selbstauskunft

secuvera:
Cybersicherheit. Nachhaltig.

Fazit

Fazit

secuvera:
Cybersicherheit. Nachhaltig.

Nicht warten, starten

T.P.S.S.E. Qualifizierung um die Fragestellung des CRA ergänzen?

secuvera:
Cybersicherheit. Nachhaltig.

Vielen Dank!
Thank you!

secuvera GmbH – 07032/97580

hello@secuvera.de

www.secuvera.de

secuvera GmbH
Siedlerstraße 22-24
71126 Gäufelden