Wie der Cyber Resilience Act die CE-Kennzeichnung beeinflusst

Im Rahmen dieser Verordnung wird Cybersicherheit zu einer **verpflichtenden Anforderung für die CE-Kennzeichnung**. Hersteller müssen nachweisen, dass ihre Produkte den neuen regulatorischen Sicherheitsstandards entsprechen und ein angemessenes **Schwachstellenmanagement** im Unternehmen etabliert ist.

Mit dem Inkrafttreten des **Cyber Resilience Act (CRA)** führt die Europäische Union verbindliche Cybersicherheitsanforderungen für **Produkte mit digitalen Elementen** ein. Ziel dieser Anforderungen ist es, die Resilienz gegenüber Cyberangriffen zu erhöhen und verlässliche digitale Services bereitzustellen.

Der CRA baut auf dem etablierten CE-Kennzeichnungsprozess auf, ergänzt diesen jedoch um spezifische Anforderungen im Bereich Cybersicherheit. Hersteller müssen nun nicht nur herkömmliche **Anforderungen an Sicherheit und Umweltschutz** erfüllen, sondern auch die **Cybersicherheitsvorgaben** des CRA – etwa sichere Software-Updates und Maßnahmen zum Risikomanagement.

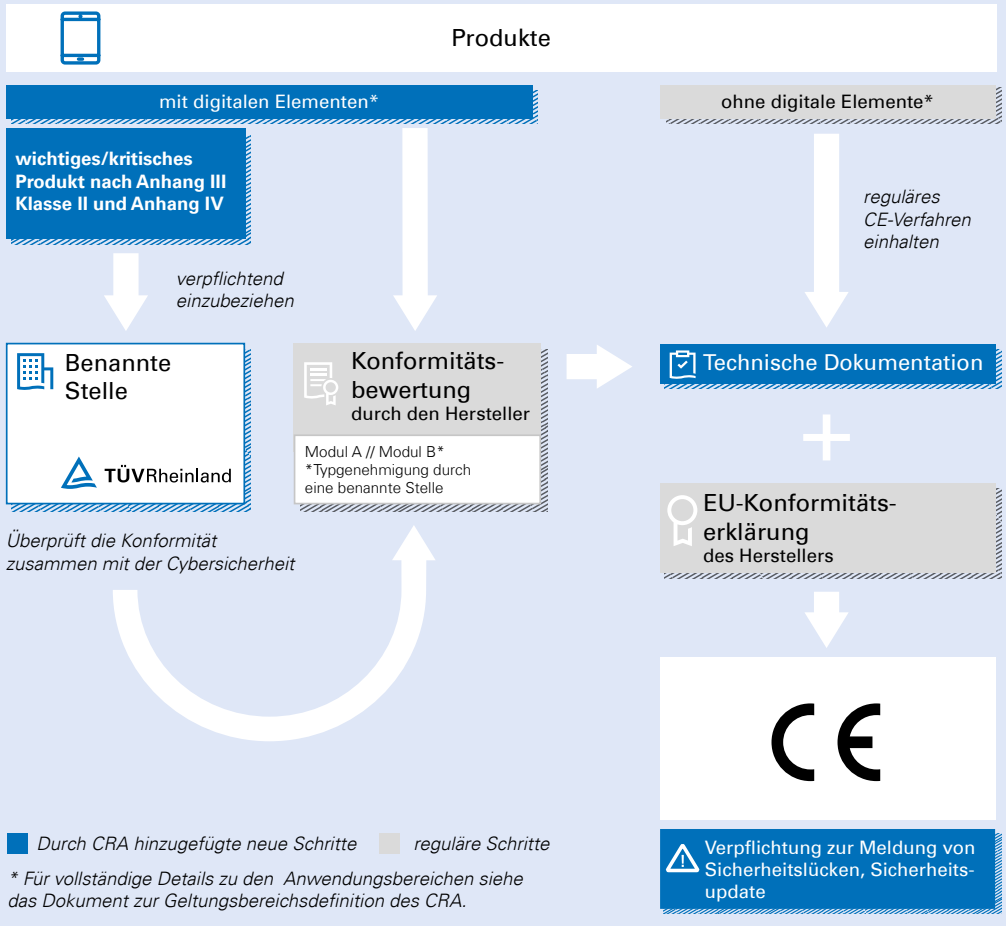
RECHTLICHE HINWEISE:
während des gesamten Prozesses zu beachten

EU-weite Anforderungen

- Wesentliche Anforderungen
- Konformitätsvermutung
  - Harmonisierte Normen
  - Gemeinsame Spezifikationen
  - Cybersicherheitssystem

§ Wichtige EU-Rechtsvorschriften

- Vorschlag 2022/0272/COD Cyber Resilience Act
- Verordnung 2019/881 Cybersecurity Act
- Vorschlag 2020/0359/COD NIS-2-Richtlinie
- Verordnung 765/2008 CE-Kennzeichnung
- Konformitätsbewertungsverfahren gemäß Verordnung 768/2008/EC



* Für vollständige Details zu den Anwendungsbereichen siehe das Dokument zur Geltungsbereichsdefinition des CRA.

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Köln
service@i-sec.tuv.com
www.tuv.com/cra_de

ONLINE-KONTAKT

TÜVRheinland®
Genau. Richtig.