



Cyber Resilience Act

**Neue EU Sicherheitsstandards für
Produkte mit digitalen Komponenten**

HIER REGISTRIEREN

12. Mai 2026

10 – 12 und 13 - 15 Uhr MEZ

Online-Training

Meetingplattform Zoom



Wer ist betroffen?

- Hersteller, Importeure und Händler von Produkten mit digitalen Komponenten, die in der EU hergestellt, importiert oder vertrieben werden. Betroffen sind Geräte, die mit dem Internet verbunden sind oder digitale Daten verarbeiten können, einschließlich vieler Haushaltsgeräte.
- Maschinen- und Anlagenbauunternehmen

Follow us on





Zielgruppe

- Geschäftsleitung von Produktions-, Zuliefer- und Handelsunternehmen
- Einkauf & Import-Exportmanagement
- Rechts- und Complianceabteilungen in Industrie und Handel
- Maschinen- und Anlagenbauunternehmen

Hintergrund

Die Bedeutung vernetzter Geräte nimmt laufend zu. Aus diesem Grund setzt die EU mit dem Cyber Resilience Act neue Standards für die Cybersicherheit von Produkten mit digitalen Komponenten.

Produzenten müssen sicherstellen, dass ihre Produkten den Anforderungen entsprechen. Händler dürfen nur konforme Produkte verkaufen, müssen diese Konformität dokumentieren (Konformitätserklärung) und die Nachverfolgbarkeit gewährleisten. Die Nichteinhaltung kann zu hohen Geldstrafen (15 Mio Euro/2,5% des Jahresumsatzes), Marktzugangsbeschränkungen, Produktrückrufen und Imageschäden führen.

Unser Experte

Michael Krausz studierte Physik, Informatik und Rechtswissenschaften in Wien und den USA, ist ausgebildeter Berufsdetektiv und Buchautor zum Thema Behandlung von Sicherheitsvorfällen. Er hat seit 1998 Kunden in 32 Ländern auf 4 Kontinenten bei der Vorbeugung und Behandlung schwerer und schwerster extern oder intern ausgelöster Sicherheitsvorfälle unterstützt. Widmet sich seit 2002 besonders der Vorbeugung von Vorfällen durch die Implementierung effektiver sowie effizienter Informationssicherheitsmanagementsysteme in komplexen Governance-Umgebungen (ISO 27001, COBIT, SOC 2, NIS/NIS-2, DORA, CRA, KRITIS, sonstige Multi-Standard Umgebungen) sowie der Verhandlungsführung und Unterstützung des Executive Managements und der IT im Ernstfall.

Das Wesentliche

- Wer ist in welchem Umfang betroffen? Hersteller vs. Importeur vs. Händler
- Anwendungsfristen (Juni/Sept 26)
- Pflichten nach dem CRA
- CRA erfüllen
 - ISO 27001
 - „freeform“
 - Checkliste zur Erfüllung
- CRA mit bestehenden Standards in Einklang bringen
- Compliance-Effizienzpotentiale heben
- Effektivität & Effizienz von Maßnahmen dauerhaft sicherstellen
- Strafbestimmungen



Cyber Resilience Act: Neue EU Sicherheitsstandards für Produkte mit digitalen Komponenten

12. Mai 2026

10 – 12 und 13 - 15 Uhr MEZ, Online

HIER REGISTRIEREN

Teilnahmegebühr pro Person

€ 405,00 + 20% USt.

inkl. elektronischen Trainingsunterlagen, Teilnahmezertifikat

Ermäßigter Preis für ICC Austria Mitglieder:

€ 324,00 + 20% USt.

Erhalten Sie 10% Rabatt p. P. bei zeitgleicher Buchung ab 3 Teilnehmenden eines Unternehmens pro Online-Training Termin !

Technische Voraussetzung

Internetfähiger Rechner/Laptop/Tablet oder Smartphone.

Das Online-Training wird über Zoom abgehalten. Sollte Ihr Unternehmen Zoom nicht standardmäßig nutzen, ist dennoch eine Teilnahme möglich. Bei Fragen wenden Sie sich bitte an Ihre hauseigene IT oder auch gerne direkt an uns.

Sie erhalten 3 Werktage vor Beginn den Link und die Zugangsdaten zur Teilnahme an der Onlineschulung.