

Einladung zum FokusTalk

Cyber Resilience Act

Was jetzt auf Unternehmen zukommt.

Dienstag, 22. September 2026, Beginn 17:00 Uhr
WIFI Klagenfurt, Europaplatz 1, Raum B001 Orangerie (Parterre)

DER CYBER RESILIENCE ACT KOMMT – SIND IHRE KUNDEN UND PRODUKTE BEREIT?

Mit dem Cyber Resilience Act (CRA) schafft die Europäische Union erstmals einheitliche Cybersicherheitsanforderungen für Produkte mit digitalen Elementen. Für Hersteller und Anbieter von Software, vernetzten Geräten und digitalen Lösungen ergeben sich daraus neue Pflichten – von Security by Design über Schwachstellenmanagement bis hin zur CE-Kennzeichnung.

Gerade IT-Dienstleister, Softwareentwickler und Beratungsunternehmen werden künftig verstärkt gefordert sein, ihre Kunden bei der Umsetzung der neuen Anforderungen zu begleiten. Wer die Auswirkungen des CRA frühzeitig versteht, kann nicht nur Compliance sicherstellen, sondern auch neue Beratungs- und Geschäftspotenziale erschließen. Erste Regelungen greifen bereits ab 11. September 2026.

In unserem Fokustalk zeigt **Michael Jesse** anhand von drei anonymisierten Praxisfällen, wie sich die Anforderungen des Cyber Resilience Act je nach Produktkategorie unterscheiden und welche konkreten Maßnahmen Unternehmen ergreifen müssen.

PROGRAMM

- **Begrüßung**, Einleitung und Moderation – **Walter Wratschko**, Leiter des UBIT-Arbeitskreises Datenschutz
- **Praxisvortrag**: Cyber Resilience Act – Drei Praxisfälle, drei Produktkategorien, konkrete Umsetzung – **Michael Jesse**

Mag. Michael JESSE
LL.M., CEMS MIM
Tech Law & Digital
Regulation Advisor



Anhand von drei typischen Unternehmensbeispielen werden die Anforderungen des CRA verständlich und praxisnah erläutert:

Praxisfall 1: Deploybare Wartungssoftware

Ein Unternehmen entwickelt eine lokal installierbare Wartungssoftware für Produktionsunternehmen. Dieses Beispiel zeigt die Anforderungen an ein Standardprodukt nach dem Cyber Resilience Act.

Praxisfall 2: Fitness- und Notfall-Wearable

Ein Unternehmen entwickelt eine vernetzte Armbanduhr mit App und Cloud-Anbindung zur Aktivitäts- und Gesundheitsüberwachung. Das Produkt ist voraussichtlich als wichtiges Produkt der Klasse I einzustufen und unterliegt erweiterten Anforderungen.

Praxisfall 3: Smart-Meter-Sicherheitsgateway

Ein Unternehmen entwickelt ein Gateway zur sicheren Anbindung intelligenter Stromzähler an Energieversorger. Aufgrund seiner sicherheitskritischen Funktion gilt es als kritisches Produkt und muss besonders hohe Anforderungen erfüllen.

Für jeden Praxisfall wird aufgezeigt:

- Wie Produkte richtig eingestuft werden
- Welche Cybersecurity-Anforderungen zu erfüllen sind
- Welche Dokumentation erforderlich ist
- Welche Konformitätsverfahren anzuwenden sind
- Wie der Weg zur CE-Kennzeichnung aussieht

FRAGEN UND DISKUSSION

AUSKLANG UND NETWORKING

Statt abstrakter Gesetzestexte erhalten Sie konkrete Einblicke in die praktische Umsetzung und erfahren, welche Auswirkungen der CRA auf unterschiedliche Unternehmen und Produkte hat.

Wir freuen uns auf einen spannenden Austausch!

Marc Gfrerer
SIC Vorsitzender

Martin Zandonella
UBIT-Fachgruppenobmann

[Anmeldung hier. >>](#)