Cyber Resilience Act für Produkthersteller und Entwickler.

Cybersichere Produkte während des gesamten Produktlebenszyklus.

Seminar	3 Termine verfügbar	Teilnahmebescheinigung
Präsenz / Virtual Classroom	8 Unterrichtseinheiten	Online durchführbar

Seminarnummer: 31779

Stand: 08.07.2026. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/31779

Der EU Cyber Resilience Act (CRA) ist eine EU-Verordnung und gilt für Produkte mit digitalen Elementen, die auf den europäischen Markt gebracht werden. Die CRA legt verbindliche Anforderungen für alle auf dem EU-Markt erhältlichen vernetzten Produkte fest, angefangen bei preisgünstigen Verbraucherprodukten bis hin zu B2B-Software und komplexen High-EndIndustriekomponenten und -systemen.

Hauptziel dieser Verordnung ist die Gewährleistung der Produktsicherheit während des gesamten Produktlebenszyklus, einschließlich Entwurf, Entwicklung, Produktion und Wartungspraktiken wie Sicherheitsupdates. Darüber hinaus legt sie klare und verbindliche Verantwortlichkeiten für Hersteller, Importeure und Händler fest.

Hersteller müssen Konformitätsbewertungsverfahren (Conformity Assessments) durchlaufen, um die Konformität ihrer Produkte mit dem CRA nachzuweisen. Auch Importeure und Händler müssen nachweisen, dass die von ihnen auf den Markt gebrachten Produkte den Anforderungen der CRA entsprechen. Bei Nichteinhaltung dürfen die Produkte nicht auf den Markt gebracht werden, und den Wirtschaftsakteuren drohen außerdem erhebliche Geldstrafen.

Dieser TÜV Rheinland-Workshop vermittelt das notwendige Wissen, um die Anforderungen der CRA erfolgreich zu erfüllen und damit die Cybersicherheit der entwickelten Produkte zu verbessern. Details, Zeitpläne und praktische Ansätze werden von unseren erfahrenen TÜV Rheinland-Experten/Trainern erläutert, damit die Teilnehmer dieses Wissen in ihren Arbeitsalltag übertragen können.

Nutzen

- Know-how: Sie erhalten notwendige und fundierte Informationen, um die gesetzlichen Verpflichtungen und Anforderungen umzusetzen, um damit die Konformität Ihrer Produkte mit CRA zu erzielen. Vertiefen Sie Ihr Wissen und erfahren Sie Einzelheiten über die Anforderungen der Normen der IEC 62443-Reihe und Normen wie ETSI EN 303 645, IEC 30111 und IEC 29147, die alle die CRA betreffen.
- Lernen Sie von Experten: Details, Zeitabläufe und praktische Vorgehensweisen werden von unseren
- erfahrenen TÜV Rheinland-Experten/Trainern erläutert, damit Sie dieses Wissen in ihren Arbeitsalltag umsetzen können.

Zielgruppe

Hersteller von Produkten mit digitalen Elementen, Importeure, Exporteure, Software-Anbieter.

Voraussetzungen

Die Teilnahme an diesem Workshop erfordert keine besonderen Vorkenntnisse und ist für Anfänger und erfahrene Anwender gleichermaßen geeignet.

Abschluss

Teilnahmebescheinigung

Teilnahmebescheinigung des TÜV Rheinland Industrie Services.

Inhalte des Seminars

Einführung Cyber Resilience Act (CRA) & Anwendungsbereich

- EU-Cybersicherheit Strategie
- CE-Kennzeichnungskonzept / Regeln des neuen Konzepts
- Anwendungsbereich der CRA
- Produkte außerhalb des Anwendungsbereichs
- Zeitplan für die Anwendung und Übergangsbestimmungen
- Anwendungsbeispiele

- Inverkehrbringen älterer Produkte
- Produktaustausch/Ersatzteile
- Beziehungen zu anderen EU-Verordnungen für Produkte (MVO, RED, etc.)

Konformitätsbewertungsverfahren

- Anforderungen für Produkte mit digitalen Elementen
- Produktkategorien
- Produktklassifizierung
- Konformitätsbewertungsverfahren
- Konformität mit den Anforderungen
- EU-Konformitätserklärung und CE-Kennzeichnung
- Marktüberwachung und Durchsetzung
- Aufgaben und Verpflichtungen
- Pflichten der Hersteller
- Pflichten von Importeuren und Händlern
- Bevollmächtigter Vertreter
- Sanktionen

Sicheres Design – Secure Design

- Bedrohungsmodell
- Lebenszyklus der sicheren Produktentwicklung
- Spezifikationen von Sicherheitsanforderungen
- Typische Sicherheitsanforderungen
- Beispiele für Bedrohungen
- Softwarearchitekturentwurf und Modelle
- Datenressourcen
- Sichere Kodierung

Technische Anforderungen

- Mechanismen zur Erreichung und zum Nachweis der Konformität
- Beispiele für mögliche Probleme, die durch Nichtkonformität verursacht werden

Anforderungen zum Umgang mit Schwachstellen

- Gewährleistung der Sicherheit vom Markteintritt bis zum Ende der Nutzungsdauer
- Identifizierung und Dokumentation von Schwachstellen
- Software-Bill of Materials (SBOM)
- Meldung von Vorfällen
- Unterstützung im Lebenszyklus
- Risikobewertungen und Dokumentation
- Sicherheitstests
- Öffentliche Bekanntgabe behobener Schwachstellen

Referenzierte Normen für CRA

- Harmonisierte Normen und Stand der Normung IEC 62443
- ETSI EN 303 645
- ISO 2700x
- IEC 30111
- IEC 29147

Offene Quelle

- Risiko und Management von Open-Source-Software
- Pflichten der Verwalter von Open-Source-Software
- Sicherheitsbescheinigung für freie und quelloffene Software

Technische und Benutzerdokumentation

- Anweisungen für den Benutzer
- Technische Dokumentation

CRA-Einhaltung

- Anleitung zur Umsetzung der CRA-Anforderungen
- Empfehlungen

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/31779 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.