✓ Durchführung gesichert!

Cyber Resilience Act (CRA) erfolgreich umsetzen

Erfüllen Sie die neuen EU-Anforderungen an Cybersicherheit – praxisnah, rechtssicher und mit klarem Wettbewerbsvorteil

Beginn:
13.07.2026 - 09:00 Uhr

Ende:
13.07.2026 - 16:30 Uhr

Dauer:
1,0 Tag

weitere Termine

Flex: Ostfildern oder Online

Veranstaltungsnr.: **36356.00.002**

Leitung

Dr. Thomas Liedtke

Präsenz oder Online
EUR 590,00
(MwSt.-frei)

Mitgliederpreis
EUR 531,00
(MwSt.-frei)

in Zusammenarbeit mit:

GESELLSCHAFT FÜR INFORMATIK

BESCHREIBUNG

CHIP Herausragend Programmierung
Analyse von 185 IT-Weiterbildern November 2025
TAE
Unabhängige Tests seit 1978
chip.de/itweiterbilder

Warum sollten Sie dieses Seminar besuchen?

Cybersicherheit ist längst keine Kür mehr – sie entscheidet über die Zukunftsfähigkeit Ihrer Produkte und Ihres Unternehmens. Der neue **EU Cyber Resilience Act (CRA)** verpflichtet Hersteller, Importeure und Händler von Produkten mit digitalen Elementen zu umfassenden Sicherheitsmaßnahmen. Doch was bedeutet das für Sie konkret?

Vielleicht fragen Sie sich:

- Welche Anforderungen muss mein Produkt erfüllen, um rechtssicher in Verkehr gebracht zu werden?
- Wie setze ich Risiko-Assessments praxisnah und effizient um?
- Welche Prozesse brauche ich, um Meldepflichten zuverlässig einzuhalten?

Genau hier setzt dieses Seminar an. Sie erfahren, wie Sie die gesetzlichen Vorgaben nicht nur erfüllen, sondern auch für sich nutzen. Mit dem richtigen Vorgehen steigern Sie Ihre Compliance, reduzieren Haftungsrisiken und stärken gleichzeitig das Vertrauen Ihrer Kunden und Partner.

Kurz: Sie sichern sich **Rechtssicherheit, Wettbewerbsfähigkeit und Zukunftsvorsprung**.

Ziel der Weiterbildung
Was lernen Sie konkret?

In diesem Seminar arbeiten Sie praxisnah an den zentralen Fragen rund um den Cyber Resilience Act:

- **Klarheit über Anforderungen**: Sie verstehen, welche Produktkategorien betroffen sind und welche Pflichten für Hersteller, Importeure und Händler gelten.
- **Risikobasierte Cybersicherheit umsetzen**: Sie lernen Methoden für Risiko-Assessments kennen – abgestimmt auf die Kritikalität Ihrer Produkte.
- **Effiziente Prozesse gestalten**: Sie entwickeln praxistaugliche Abläufe für Incident-Management, Schwachstellen-Handling und kontinuierliche Sicherheitsüberwachung.
- **Meldepflichten sicher erfüllen**: Sie wissen, welche Fristen, Inhalte und Zuständigkeiten gelten und wie Sie diese zuverlässig einhalten.
- **Synergien nutzen**: Sie verknüpfen den CRA mit NIS-2, ISO/IEC 62443, MVO und bestehenden Compliance-Strukturen.
- **Rechtliche Sicherheit gewinnen**: Sie erkennen, welche Sanktionen drohen, und erfahren, wie Sie Haftungsrisiken proaktiv reduzieren.
- **Wettbewerbsvorteile realisieren**: Sie nutzen Cybersicherheit und Konformität aktiv als Qualitäts- und Marketingfaktor.

Nach dem Seminar können Sie die Vorgaben des CRA zielgerichtet in Ihrer Organisation anwenden – und sichern sich damit einen klaren Vorsprung.

IMMER TOP!

Unser Qualitätsversprechen

Seit über 65 Jahren gehört die Technische Akademie Esslingen (TAE) mit Sitz in Ostfildern – nahe der Landeshauptstadt Stuttgart – zu Deutschlands größten Weiterbildungs-Anbietern für berufliche und berufsvorbereitende Qualifizierung im technischen Umfeld. Unser Ziel ist Ihr Erfolg. Egal ob Seminar, Zertifikatslehrgang oder Fachtagung, unsere Veranstaltungen sind stets abgestimmt auf die Bedürfnisse von Ingenieuren sowie Fach- und Führungskräften aus technisch geprägten Unternehmen. Dabei können Sie sich stets zu 100 Prozent auf die Qualität unserer Angebote verlassen. Warum das so ist?

PROGRAMM

1 | Motivation

- Ziele und Motivation des CRA
- Wer und was ist betroffen?

2 | EU Cyber Resilience Act (EU-Gesetz über Cyberresilienz)

- Überblick über die essentiellen Cybersecurity-Anforderungen gemäß Cyber Resilience Act
- EU-Vorschriften zur Gewährleistung sicherer Hardware und Software
- typische Sicherheitsrisiken von Produkten und Software mit digitalen Komponenten
- Verbraucherschutz als zentrales Ziel des CRA
- Anforderungen an Sicherheitsupdates und kontinuierliche Pflege
- Risikobewertung: Erkennen, welche Produkte cybersicher sind und wie sie sicher konfiguriert werden
- Harmonisierte Vorschriften für das Inverkehrbringen von Produkten oder Software mit digitalen Komponenten
- Rahmenwerk für Cybersicherheitsanforderungen in Planung, Design, Entwicklung und Wartung – mit Pflichten in allen Phasen der Wertschöpfungskette
- Rollen und Verantwortlichkeiten der verschiedenen Marktakteure (Hersteller, Importeure, Händler)
- Sorgfaltspflichten über den gesamten Lebenszyklus hinweg

3 | Praxisbeispiel für eine Risikoanalyse

4 | Zusammenfassung und Ausblick

- Beispiele für harmonisierte Normen, die im Entstehen sind (Agrar, Maschinen, Bahnen ...)

TEILNEHMER:INNENKREIS

Für wen ist das Seminar geeignet?

Dieses Seminar richtet sich an **Fach- und Führungskräfte**, die Verantwortung für die Entwicklung, den Import oder den Vertrieb von Produkten mit digitalen Elementen tragen.

Besonders profitieren:

- Produktmanagerinnen und -manager
- Projektleiterinnen und Projektleiter
- Qualitäts- und Compliance-Verantwortliche
- IT-Sicherheitsbeauftragte und Risikomanager
- Hersteller, Importeure und Händler

Ebenso wertvoll ist das Seminar für Juristinnen und Juristen, Auditorinnen und Auditoren, Beraterinnen und Berater sowie technische Redakteurinnen und Redakteure, die Cybersicherheits- und Meldepflichten im Rahmen des CRA umsetzen oder begleiten.

REFERENT:INNEN

Dr. Thomas Liedtke

Dr. Thomas Liedtke ist
- seit vielen Jahren beratend tätig für funktionale Sicherheit, Informations- und Produktsecurity. Er ist Mitglied der deutschen DIN-AK-Spiegelgruppe, welche für die Definition ISO/SAE 21434, ISO/PAS 5112 und weitere Cybersecuritystandards verantwortlich ist
- Mitglied des intacs Advisory Boards und Leiter der SPICE Cybersecurity Arbeitsgruppe Leiter der ZVEI Arbeitsgruppe Datensicherheit im Automobil
- Leadauditor für CSMS; ISMS; TISAX
- Berater für die Implementierung der Cybersecurity in Unternehmen Publikationen
- Informationssicherheit: Möglichkeiten und Grenzen; SpringerLink publisher: link.springer.com/book/10.1007/978-3-662-63917-7
- The New Cybersecurity Challenges and Demands for Automotive Organisations and Projects – an Insight View link.springer.com/chapter/10.1007/978-3-031-42307-9_21

Weitere Veranstaltungen

Cyber-Sicherheit für kritische Infrastrukturen: NIS2 & CER verstehen und umsetzen

Intelligente Systeme in der Industrie: Architektur, Einsatz und Wirtschaftlichkeit

Einführung in die Kryptographie: Methoden und praktische Anwendungen

Sicherheitsgerichtete Systeme entwickeln

VERANSTALTUNGSORT UND HOTEL

Technische Akademie Esslingen
An der Akademie 5
73760 Ostfildern

Anfahrt
Die TAE befindet sich im Südwesten Deutschlands im Bundesland Baden-Württemberg – in unmittelbarer Nähe zur Landeshauptstadt Stuttgart. Unser Schulungszentrum verfügt über eine hervorragende Anbindung und ist mit allen Verkehrsmitteln gut und schnell zu erreichen.

Hotelübernachtung benötigt?

Über den nachfolgenden Link finden Sie nahegelegene Hotels in direkter Umgebung zu TAE-Konditionen:

Hotelbuchung

GEBÜHREN UND FÖRDERMÖGLICHKEITEN

Die Teilnahme beinhaltet Verpflegung (vor Ort) sowie ausführliche Unterlagen.

Preis:
Die Teilnahmegebühr beträgt:
590,00 € (MwSt.-frei) vor Ort
590,00 € (MwSt.-frei) pro Teilnehmer live online

Fördermöglichkeiten:
Für den aktuellen Veranstaltungstermin steht Ihnen die ESF-Fachkursförderung leider nicht zur Verfügung.

Für alle weiteren Termine erkundigen Sie sich bitte vorab bei unserer Anmeldung.

Andere Bundesland-spezifische Fördermöglichkeiten finden Sie hier.

Inhouse Durchführung:
Sie möchten diese Veranstaltung firmenintern bei Ihnen vor Ort durchführen? Dann fragen Sie jetzt ein individuelles Inhouse-Training an.

Weitere Termine und Orte

Datum	Lernsetting & Ort	Preis
Beginn: 27.11.2026 Ende: 27.11.2026	Flex: Ostfildern oder Online	EUR 590,00
Datum	**Lernsetting & Ort**	**Preis**
Beginn: 15.03.2027 Ende: 15.03.2027	Flex: Ostfildern oder Online	EUR 590,00