Fraunhofer ACADEMY

Cyber-Resilienz für den Bereich Automatisierungstechnik

Anforderungen und neue Chancen durch den Cyber Resilience Act (CRA)

Teilnehmende erfahren, wie sie die Anforderungen des Cyber Resilience Acts (CRA) in der Automatisierungstechnik umsetzen können. Der Kurs bietet praxisnahe Einblicke in gesetzliche Vorgaben, Sicherheitsstrategien und Techniken, um die Cyber-Resilienz zu steigern und ihre Produkte und Dienstleistungen optimal abzusichern.

Cyber Resilience Act: Anforderungen erfüllen und Sicherheitsfeatures als Wettbewerbsvorteil nutzen

Wie können Unternehmen die neuen Anforderungen des Cyber Resilience Act (CRA) effizient umsetzen und zugleich ihre Marktposition stärken?

Dieser praxisnahe Kurs vermittelt nicht nur die gesetzlichen Vorgaben, sondern zeigt, wie zusätzliche Sicherheitsfeatures einen Wettbewerbsvorteil schaffen können.

Die Teilnehmenden erhalten einen umfassenden Überblick über die rechtlichen und normativen Grundlagen sowie konkrete Handlungsanleitungen für ihre spezifischen Produkte.

Besonderes Augenmerk liegt darauf, wie über die gesetzlichen Mindestanforderungen hinausgehende Sicherheitsfeatures als Wettbewerbsvorteil genutzt werden können.

Kursdetails auf einen Blick

- Für **Fachkräfte, Spezialist*innen und Führungskräfte**
- **Offene Schulung** oder **Inhouse Training**
- Dauer: **2 Tage**
- Format: **Präsenz oder Online**
- Kosten: 1.600,00 Euro (USt.-befreit gem. § 4 Nr. 22a UStG)

KRITIS-Pflichten verstehen und Cyber-Resilienz praxisnah umsetzen

Neben den regulatorischen Anforderungen behandelt das Seminar die Rolle von KRITIS-Betreibern und die daraus resultierenden Pflichten und Bedürfnisse für Komponentenhersteller. Dabei wird detailliert erarbeitet, welche technischen Maßnahmen und Werkzeuge notwendig sind, um Cyber-Sicherheit und Resilienz in Produkte zu integrieren.

Durch praxisorientierte Übungen wird das erlernte Wissen direkt anwendbar. Die Teilnehmenden arbeiten mit Softwarelösungen für Assetmanagement und Angriffserkennung sowie mit Methoden zur Absicherung von Entwicklungsprozessen.

So können sie die neuen Anforderungen effizient und vorausschauend in ihre Unternehmensstrategie integrieren.

Nach dem Seminar können Sie:

- **notwendige Maßnahmen** für Ihre Produkte und Services aus der aktuellen Gesetzeslage **ableiten.**
- eine geeignete **Plattform für Asset Management auswählen**, bedienen und die **Rolle der Komponenten** dabei **einschätzen**.
- **Software-Tools zur Angriffserkennung** gezielt auswählen sowie **Schwachstellenmanagement und Serviceleistungen** zur Kundenbindung strategisch **nutzen**.

Kursinhalte

Das Spektrum der behandelten Themen umfasst:

- Gesetzeslage CRA und zugehörige Normen
- Asset Management
- Schutzmaßnahmen und Cybersecurity
- Angriffserkennung
- Schwachstellenmanagement
- Business Continuity

Zugangsvoraussetzung:

Keine.
Von Vorteil: Grundlagen Cybersicherheit Programmierung und Entwicklung von industrieller Elektronik

Alle Kursdetails und die Anmeldung finden Sie hier:

https://s.fhg.de/CRA-Automatisierungstechnik

Fachlicher Ansprechpartner am Fraunhofer IOSB-INA

Burkhard Gilles
Tel. +49 5261 9429022
burkhard.gilles@iosb-ina.fraunhofer.de

Fraunhofer IOSB-INA
Campusallee 1
32657 Lemgo

Lernlabor
Cybersicherheit