Cyber Resilience Act & EU-Produkthaftung in der Praxis (Präsenz)

Neue Cyber-Security-Anforderungen ab 2026 für Software, KI und vernetzte digitale Geräte in der EU

Cyber Resilience Act (CRA), NIS 2 und die neuen EU-Produkthaftungsregeln für Software und Hochrisiko-KI-Systeme stellen Unternehmen vor erhebliche rechtliche und praktische Herausforderungen in Sachen Cybersicherheit. Der Anwendungsbereich des CRA auf Produkte ist sehr weit. Hinzu kommt, dass Hersteller künftig für Open-Source-Komponenten verantwortlich sind. Die strengen Meldepflichten bei bestimmten Cybersicherheitsvorfällen gelten schon ab Herbst 2026, ab Dezember 2027 ist dann der Vertrieb von Software oder vernetzten Geräten nur noch mit CE-Kennzeichen als Siegel für Cybersicherheit zulässig. Das Seminar bietet einen kompakten, praxisnahen und fundierten Einstieg in diese Vorgaben. Im Fokus stehen Produkte von Unternehmen, die Software, Apps oder KI entwickeln, vertreiben oder importieren, ebenso aber Hardware und andere Geräte mit jeglichen digitalen Komponenten. Der Anwendungsbereich ist sehr weit. Behandelt werden aktuelle Informationen der EU (Meldestellen, harmonisierte Standards) und zentrale Inhalte des CRA wie Security by Design, Konformitätsverfahren, Produktklassen, Sicherheitsanforderungen, Meldepflichten und Reaktionszeiten, Software-Stücklisten (SBOM) und technische Informationspflichten. Zudem wird das Zusammenspiel von CRA, Produktsicherheit und EU-Produkthaftung und -Mängelhaftung besprochen. Das Seminar befähigt dazu, CRA und Haftungsumfang zu verstehen, auf eigene Praxisfälle anzuwenden und neue Pflichten in bestehende Prozesse zu integrieren. Beispielfälle und Fragen aus der Praxis werden gemeinsam diskutiert.

Inhalte

Grundlagen
- Einführung in die Ziele von CRA, NIS 2 und der EU-Produkthaftungs-Richtlinie, um Rahmenbedingungen und Hintergründe besser zu verstehen, wie die digitale Souveränität in der EU.
- Reichweite des CRA in Abgrenzung zu NIS 2 und dem AI Act.
- Einordnung von Software und Produkten mit digitalen Elementen in Risikoklassen nach dem Cyber Resilience Act (CRA) und die damit verbundenen Pflichten.
- Verantwortliche Akteur:innen.
- Verantwortliche im Unternehmen zur Umsetzung des CRA in die Praxis.

Software Bill of Materials (SBOM)
- Inhalte, Format und Bereitstellung der Softwarestücklisten (SBOM).
- Lösungsansätze und Standards wie die BSI-Vorgaben zur Gewährleistung von Transparenz und Erhöhung der Sicherheit in der Software-Lieferkette (Software Supply Chain Security).

Sicherheitsanforderungen und Cybersecurity-Maßnahmen für Software und Produkte mit digitalen Elementen im CRA
- Inhalt von Cybersecurity-Strategien von der Entwicklung bis zum Inverkehrbringen und in der Lieferkette, OSS Compliance.
- Security by Design, Update-Pflichten über den gesamten Produktlebenszyklus von Software hinweg.
- Notwendigkeit eines kontinuierlichen Sicherheitsmanagements.
- Gewährleistung der Cybersicherheit der digitalen Komponenten, von IoT-Produkten und von funktioneller Sicherheit durch Security by Design und strenge Meldepflichten.
- Was bedeuten die Updatepflichten von fünf Jahren für die Cybersicherheit von Produkten in der Praxis?

Konformitätsbewertungsverfahren und CE-Kennzeichnung
- Konformitätsbewertungsverfahren.
- Praktische Umsetzung der CE-Kennzeichnungspflicht für die Produkte.

Haftungsumfang des CRA für Produkte mit Open-Source-Software-Code, inklusive Lizenzmanagement und Haftungsausnahmen
- Lösungsansätze zum sicheren Umgang mit Open-Source-Software in Produkten in der Lieferkette.
- Verantwortlichkeiten, Ausnahmen, gesetzliche und vertragliche Haftung.

Meldepflichten bei Sicherheitsvorfällen
- Überblick über die Meldepflichten und Reaktionszeiten bei Sicherheitsvorfällen, um Sanktionen vorzubeugen.

Umsetzungsfristen, Rechtsfolgen bei Verstößen

- Fristen für die Umsetzung der neuen Anforderungen und die Anbringung des CE-Kennzeichens.
- Sanktionen, Bußgelder und andere Konsequenzen bei Verstößen gegen die neuen Regeln.
- Auswege und Ausnahmen.

EU-Produkthaftung für Software

- Erläuterung der verschuldensunabhängigen EU-Produkthaftung für Software, digitale Technologien und Künstliche Intelligenz.
- Änderungen durch die geplante EU-Produkthaftungsrichtlinie bei fehlerhafter Software und Abgrenzung zur Mängelhaftung.
- Reichweite der neuen Regelungen.
- Verantwortliche und Umfang der Haftung.
- Lösungsansätze zur Haftungsreduktion.
- Produkthaftung für Hochrisiko-KI-Systeme gemäß der KI-Verordnung und dem CRA.

Lernumgebung

In deiner Online-Lernumgebung findest du nach deiner Anmeldung nützliche Informationen, Downloads und Extra-Services zu dieser Qualifizierungsmaßnahme.

Dein Nutzen

- Praxistransfer: Verständnis der EU-Vorgaben und Anwendung des CRA auf eigene Produkte in der Praxis.
- Stets aktuell informiert über die neuen Vorgaben der EU zum CRA.
- Austausch mit anderen Unternehmen und Teilnehmer:innen zu konkreten Umsetzungs- und Anwendungsfragen.
- Wertvolle neue Lösungsansätze für die Umsetzung durch Diskussionen.
- Juristische Vorgaben der EU anwenden, Rechtsunsicherheiten verstehen und damit umgehen und sie aushalten lernen.
- Checklisten und Handlungsempfehlungen.

Methoden

Interaktiver Vortrag mit Präsentation, Diskussion, Erfahrungsaustausch und Vernetzung der Teilnehmer:innen untereinander, Übungen und Anwendung des Erlernten in kleinen Gruppen, potenzielle Lösungswege, Anregungen, Beispiele, Diskussion individueller Praxisfragen

Teilnehmer:innenkreis

Geschäftsführer:innen, Führungskräfte, IT-Expert:innen, Entwickler:innen, Programmierer:innen, Compliance-Mitarbeiter:innen, Syndikusanwält:innen von Anbietern oder Herstellern von Software, IoT-Produkten, Hardware und anderen Technologien, die sich auf die neuen EU-Sicherheitsanforderungen von CRA, NIS 2 und der EU-Produkthaftung vorbereiten und die Risiken und Haftung minimieren möchten.

Diese Veranstaltung ist auch als Modul buchbar von:

Karrierepaket: Führen im IT-Kontext

Open Badges - Zeige auch digital, was du kannst.

Open Badges sind anerkannte, digitale Teilnahmezertifikate. Diese verifizierbaren Nachweise sind der aktuelle Standard für die Einbindung in Karrierenetzwerken wie z.B. LinkedIn.

Damit zeigst du digital, über welche Kompetenzen du verfügst.

Nach erfolgreichem Abschluss erhältst du von uns ein Open Badge.

Mehr erfahren kannst du unter:
https://www.haufe-akademie.de/seminare-lehrgaenge/trending-topics/open-badges

Referent:in

Vilma Niclas
Mich fasziniert es, juristische Laien für das IT-Recht zu begeistern. Ich liebe es, diesen die Türen zu diesem vermeintlich trockenen Wissen zu öffnen. Anhand vieler Beispiele aus meiner Beratungspraxis vermittle ich selbst schwierige juristische Inhalte anschaulich, verständlich und unterhaltsam. Als Journalistin werfe ich einen kritischen Blick auf Gesetze und Rechtsprechung.

Details zur Weiterbildung

Seminar | Präsenz

1 Tag

Termine

11.02.2027
Berlin
Veranstaltungsort
Leonardo Royal Berlin Alexanderplatz

Tage & Uhrzeit
Donnerstag, 11.02.2027
09:00 Uhr - 17:00 Uhr

Aktuelle Termine und weitere Informationen findest du unter www.haufe-akademie.de/41195

Teilnahmegebühr

€ 920,- zzgl. MwSt.
€ 1.094,80 inkl. MwSt.
Die angegebene Teilnahmegebühr beinhaltet

- ein gemeinsames Mittagessen pro vollem Seminartag,
- Pausenverpflegung und
- umfangreiche Arbeitsunterlagen.

Die Übernachtungskosten im Hotel werden von den Teilnehmenden direkt mit dem Hotel abgerechnet. Für die Hotelbuchung findest du in deiner Lernumgebung ein Reservierungsformular.

Deine Anmeldemöglichkeiten

Online: www.haufe-akademie.de/41195
E-Mail: anmelden@haufe-akademie.de

Buche deine Weiterbildung einfach und schnell online. Gib sonst bitte unbedingt den Namen des Teilnehmenden und die vollständige Rechnungsanschrift mit Telefonnummer sowie E-Mail-Adresse an.

In unserem Bereich Fragen & Antworten (FAQ) findest du alle Antworten auf die häufigsten Fragen rund um unsere Weiterbildungen:
https://www.haufe-akademie.de/faqs

Unsere ausführlichen Teilnahmebedingungen findest du auch im Internet unter www.haufe-akademie.de/agb oder im Gesamtprogramm.
Die vollständigen Datenschutzbestimmungen findest du unter www.haufe-akademie.de/datenschutz.

Cyber Resilience Act & EU-Produkthaftung in der Praxis (Live-Online)

Neue Cyber-Security-Anforderungen ab 2026 für Software, KI und vernetzte digitale Geräte in der EU

Cyber Resilience Act (CRA), NIS 2 und die neuen EU-Produkthaftungsregeln für Software und Hochrisiko-KI-Systeme stellen Unternehmen vor erhebliche rechtliche und praktische Herausforderungen in Sachen Cybersicherheit. Der Anwendungsbereich des CRA auf Produkte ist sehr weit. Hinzu kommt, dass Hersteller künftig für Open-Source-Komponenten verantwortlich sind. Die strengen Meldepflichten bei bestimmten Cybersicherheitsvorfällen gelten schon ab Herbst 2026, ab Dezember 2027 ist dann der Vertrieb von Software oder vernetzten Geräten nur noch mit CE-Kennzeichen als Siegel für Cybersicherheit zulässig. Das Seminar bietet einen kompakten, praxisnahen und fundierten Einstieg in diese Vorgaben. Im Fokus stehen Produkte von Unternehmen, die Software, Apps oder KI entwickeln, vertreiben oder importieren, ebenso aber Hardware und andere Geräte mit jeglichen digitalen Komponenten. Der Anwendungsbereich ist sehr weit. Behandelt werden aktuelle Informationen der EU (Meldestellen, harmonisierte Standards) und zentrale Inhalte des CRA wie Security by Design, Konformitätsverfahren, Produktklassen, Sicherheitsanforderungen, Meldepflichten und Reaktionszeiten, Software-Stücklisten (SBOM) und technische Informationspflichten. Zudem wird das Zusammenspiel von CRA, Produktsicherheit und EU-Produkthaftung und -Mängelhaftung besprochen. Das Seminar befähigt dazu, CRA und Haftungsumfang zu verstehen, auf eigene Praxisfälle anzuwenden und neue Pflichten in bestehende Prozesse zu integrieren. Beispielfälle und Fragen aus der Praxis werden gemeinsam diskutiert.

Inhalte

Grundlagen
- Einführung in die Ziele von CRA, NIS 2 und der EU-Produkthaftungs-Richtlinie, um Rahmenbedingungen und Hintergründe besser zu verstehen, wie die digitale Souveränität in der EU.
- Reichweite des CRA in Abgrenzung zu NIS 2 und dem AI Act.
- Einordnung von Software und Produkten mit digitalen Elementen in Risikoklassen nach dem Cyber Resilience Act (CRA) und die damit verbundenen Pflichten.
- Verantwortliche Akteur:innen.
- Verantwortliche im Unternehmen zur Umsetzung des CRA in die Praxis.

Software Bill of Materials (SBOM)
- Inhalte, Format und Bereitstellung der Softwarestücklisten (SBOM).
- Lösungsansätze und Standards wie die BSI-Vorgaben zur Gewährleistung von Transparenz und Erhöhung der Sicherheit in der Software-Lieferkette (Software Supply Chain Security).

Sicherheitsanforderungen und Cybersecurity-Maßnahmen für Software und Produkte mit digitalen Elementen im CRA
- Inhalt von Cybersecurity-Strategien von der Entwicklung bis zum Inverkehrbringen und in der Lieferkette, OSS Compliance.
- Security by Design, Update-Pflichten über den gesamten Produktlebenszyklus von Software hinweg.
- Notwendigkeit eines kontinuierlichen Sicherheitsmanagements.
- Gewährleistung der Cybersicherheit der digitalen Komponenten, von IoT-Produkten und von funktioneller Sicherheit durch Security by Design und strenge Meldepflichten.
- Was bedeuten die Updatepflichten von fünf Jahren für die Cybersicherheit von Produkten in der Praxis?

Konformitätsbewertungsverfahren und CE-Kennzeichnung
- Konformitätsbewertungsverfahren.
- Praktische Umsetzung der CE-Kennzeichnungspflicht für die Produkte.

Haftungsumfang des CRA für Produkte mit Open-Source-Software-Code, inklusive Lizenzmanagement und Haftungsausnahmen
- Lösungsansätze zum sicheren Umgang mit Open-Source-Software in Produkten in der Lieferkette.
- Verantwortlichkeiten, Ausnahmen, gesetzliche und vertragliche Haftung.

Meldepflichten bei Sicherheitsvorfällen
- Überblick über die Meldepflichten und Reaktionszeiten bei Sicherheitsvorfällen, um Sanktionen vorzubeugen.

Umsetzungsfristen, Rechtsfolgen bei Verstößen

- Fristen für die Umsetzung der neuen Anforderungen und die Anbringung des CE-Kennzeichens.
- Sanktionen, Bußgelder und andere Konsequenzen bei Verstößen gegen die neuen Regeln.
- Auswege und Ausnahmen.

EU-Produkthaftung für Software

- Erläuterung der verschuldensunabhängigen EU-Produkthaftung für Software, digitale Technologien und Künstliche Intelligenz.
- Änderungen durch die geplante EU-Produkthaftungsrichtlinie bei fehlerhafter Software und Abgrenzung zur Mängelhaftung.
- Reichweite der neuen Regelungen.
- Verantwortliche und Umfang der Haftung.
- Lösungsansätze zur Haftungsreduktion.
- Produkthaftung für Hochrisiko-KI-Systeme gemäß der KI-Verordnung und dem CRA.

Lernumgebung

In deiner Online-Lernumgebung findest du nach deiner Anmeldung nützliche Informationen, Downloads und Extra-Services zu dieser Qualifizierungsmaßnahme.

Dein Nutzen

- Praxistransfer: Verständnis der EU-Vorgaben und Anwendung des CRA auf eigene Produkte in der Praxis.
- Stets aktuell informiert über die neuen Vorgaben der EU zum CRA.
- Austausch mit anderen Unternehmen und Teilnehmer:innen zu konkreten Umsetzungs- und Anwendungsfragen.
- Wertvolle neue Lösungsansätze für die Umsetzung durch Diskussionen.
- Juristische Vorgaben der EU anwenden, Rechtsunsicherheiten verstehen und damit umgehen und sie aushalten lernen.
- Checklisten und Handlungsempfehlungen.

Methoden

Interaktiver Vortrag mit Präsentation, Diskussion, Erfahrungsaustausch und Vernetzung der Teilnehmer:innen untereinander, Übungen und Anwendung des Erlernten in kleinen Gruppen, potenzielle Lösungswege, Anregungen, Beispiele, Diskussion individueller Praxisfragen

Teilnehmer:innenkreis

Geschäftsführer:innen, Führungskräfte, IT-Expert:innen, Entwickler:innen, Programmierer:innen, Compliance-Mitarbeiter:innen, Syndikusanwält:innen von Anbietern oder Herstellern von Software, IoT-Produkten, Hardware und anderen Technologien, die sich auf die neuen EU-Sicherheitsanforderungen von CRA, NIS 2 und der EU-Produkthaftung vorbereiten und die Risiken und Haftung minimieren möchten.

Open Badges - Zeige auch digital, was du kannst.

Open Badges sind anerkannte, digitale Teilnahmezertifikate. Diese verifizierbaren Nachweise sind der aktuelle Standard für die Einbindung in Karrierenetzwerken wie z.B. LinkedIn.

Damit zeigst du digital, über welche Kompetenzen du verfügst.

Nach erfolgreichem Abschluss erhältst du von uns ein Open Badge.

Mehr erfahren kannst du unter:
https://www.haufe-akademie.de/seminare-lehrgaenge/trending-topics/open-badges

Referent:in

Vilma Niclas
Mich fasziniert es, juristische Laien für das IT-Recht zu begeistern. Ich liebe es, diesen die Türen zu diesem vermeintlich trockenen Wissen zu öffnen. Anhand vieler Beispiele aus meiner Beratungspraxis vermittle ich selbst schwierige juristische Inhalte anschaulich, verständlich und unterhaltsam. Als Journalistin werfe ich einen kritischen Blick auf Gesetze und Rechtsprechung.

Details zur Weiterbildung

Seminar | Online

1 Tag

Starttermine

17.09.2026
Live-Online
Durchführung
zoom

Modulzeiten
Donnerstag, 17.09.2026
09:00 Uhr - 17:00 Uhr

24.11.2026
Live-Online
Durchführung
zoom

Modulzeiten
Dienstag, 24.11.2026
09:00 Uhr - 17:00 Uhr

Aktuelle Termine und weitere Informationen findest du unter www.haufe-akademie.de/41197

Teilnahmegebühr

€ 920,- zzgl. MwSt.
€ 1.094,80 inkl. MwSt.

Deine Anmeldemöglichkeiten

Online: www.haufe-akademie.de/41195
E-Mail: anmelden@haufe-akademie.de

Buche deine Weiterbildung einfach und schnell online. Gib sonst bitte unbedingt den Namen des Teilnehmenden und die vollständige Rechnungsanschrift mit Telefonnummer sowie E-Mail-Adresse an.

In unserem Bereich Fragen & Antworten (FAQ) findest du alle Antworten auf die häufigsten Fragen rund um unsere Weiterbildungen:
https://www.haufe-akademie.de/faqs

Unsere ausführlichen Teilnahmebedingungen findest du auch im Internet unter www.haufe-akademie.de/agb oder im Gesamtprogramm.
Die vollständigen Datenschutzbestimmungen findest du unter www.haufe-akademie.de/datenschutz.