

Alt Gr



Cyber Resilience Act in der Anwendung

Vom Gesetz zur gelebten Compliance –
Strategien zur rechtskonformen Vorbereitung

Cyber Resilience Act in der Anwendung

Vom Gesetz zur gelebten Compliance – Strategien zur rechtskonformen Vorbereitung

Kurzbeschreibung

Der im Dezember 2024 in Kraft getretene EU Cyber Resilience Act (CRA) legt erstmals verbindliche Mindestanforderungen an die Cybersicherheit für alle Produkte mit digitalen Elementen fest, die auf dem europäischen Markt verkauft werden. Ziel ist es, das Cybersicherheitsniveau innerhalb der EU zu erhöhen und sowohl Verbraucher als auch Unternehmen besser vor Cyberangriffen und Sicherheitslücken zu schützen.

Dieser ganztägige Workshop bietet den Teilnehmenden einen praxisnahen, verständlichen Einstieg in den CRA und zeigt, wie dessen Anforderungen branchenübergreifend im Unternehmen umgesetzt werden können. Ohne spezifische Vorkenntnisse vorauszusetzen, erklärt der Workshop die rechtlichen Pflichten und organisatorischen Maßnahmen, die der CRA mit sich bringt, und legt den Schwerpunkt auf Compliance-Strategien statt technischer Details. Die Teilnehmenden erfahren, welche Verpflichtungen Hersteller, Importeure und Betreiber digitaler Produkte erfüllen müssen und wie sie ihr Unternehmen darauf vorbereiten können. Durch praxisorientierte Übungen, Fallbeispiele und Diskussionen erhalten Sie konkrete Handlungsempfehlungen und gewinnen Sicherheit im Umgang mit dem neuen Gesetz. Am Ende des Tages sind Sie gerüstet, um die CRA-Anforderungen proaktiv anzugehen und die Cyber-Resilienz sowie Compliance Ihres Unternehmens zu stärken.



Inhalte

- Rechtliche Pflichten und Verantwortlichkeiten entlang der Wertschöpfungskette
- Organisatorische Umsetzung der CRA-Vorgaben im Unternehmen
- Praxisorientierte Maßnahmen zur Compliance-Vorbereitung und –Sicherung
- Interaktiver Austausch und Networking

Was lernen Sie in diesem Seminar?

Nach dem Workshop verstehen Sie die zentralen Anforderungen des Cyber Resilience Act aus Compliance-Sicht. Sie wissen, welche rechtlichen Pflichten auf Unternehmen zukommen und welche organisatorischen Maßnahmen notwendig sind, um diesen Anforderungen strukturiert zu begegnen. Sie können einschätzen, welche Verantwortlichkeiten, Prozesse und Dokumentationspflichten im Unternehmen anzupassen sind, um eine CRA-konforme Unternehmenspraxis aufzubauen. Zudem erhalten Sie praxisnahe Impulse, wie Sie den CRA systematisch in Ihre Compliance-Strategie integrieren.

Cyber Resilience Act in der Anwendung

Vom Gesetz zur gelebten Compliance – Strategien zur rechtskonformen Vorbereitung

Zielgruppe

Der Workshop richtet sich **branchenübergreifend** an Fach- und Führungskräfte, die sich auf die Anforderungen des Cyber Resilience Act vorbereiten möchten (kein spezifisches Vorwissen erforderlich). Insbesondere angesprochen sind:

- Compliance-Beauftragte und Juristinnen und Juristen, die regulatorische Vorgaben umsetzen und die Einhaltung neuer Cybersecurity-Vorschriften sicherstellen müssen.
- Qualitätsmanager und Risk Manager, die interne Prozesse und Kontrollen anpassen, um den CRA-Anforderungen gerecht zu werden.
- Führungskräfte im Bereich IT, Technik oder Geschäftsführung, die einen strategischen Überblick über kommende Cybersecurity-Gesetze benötigen, um ihr Unternehmen zukunftssicher aufzustellen.
- Berater und Dienstleister im Bereich IT-Sicherheit und Compliance, die ihre Kunden bei der Vorbereitung auf den CRA unterstützen möchten.

Didaktischer Aufbau

- Fachinput: Vermittlung der Inhalte in verständlichen Sessions (Präsentation der gesetzlichen Grundlagen, Pflichten und Best Practices) untermauert mit Praxisbeispielen.
- Interaktive Diskussionen: Gezielte Frage-Antwort-Runden und moderierte Gespräche nach jedem Themenblock ermöglichen den Erfahrungsaustausch und die Klärung von Verständnisfragen.
- Praxisnahe Gruppenarbeiten: Die Teilnehmenden bearbeiten Fallbeispiele in Kleingruppen, um das Gelernte direkt anzuwenden. Durch diese gruppenbasierten Übungen wird theoretisches Wissen in praktisches Handeln übertragen.
- Reflexion und Transfer: Gemeinsame Reflexionsphasen (z.B. beim Erarbeiten des Maßnahmenplans) helfen den Teilnehmenden, die Seminarinhalte auf die eigene Unternehmenspraxis zu übertragen und konkrete nächste Schritte zu planen.
- Unterstützungsunterlagen: Die Teilnehmenden erhalten begleitende Materialien (Präsentationsfolien, Checklisten, weiterführende Links), die es ihnen erleichtern, die Workshop-Inhalte nach dem Tag eigenständig nachzuvollziehen und im Betrieb umzusetzen.

Cyber Resilience Act in der Anwendung

Vom Gesetz zur gelebten Compliance – Strategien zur rechtskonformen Vorbereitung



Zusatzinformationen

- Der Workshop findet im kleinen Kreis mit einer Maximalteilnehmerzahl von **15 Personen** statt. Die Mindestteilnehmerzahl beträgt 5.
- Der Online-Workshop wird mit Zoom durchgeführt. Systemvoraussetzungen und unterstützte Betriebssysteme können Sie [hier](#) einsehen. Für die Einwahl in Zoom über die verschiedenen Anwendungen (Desktop Client, App oder Web-Client) bietet Ihnen [diese Tabelle](#) einen zusätzlichen Vergleich zu den Eigenschaften.
- Die Bitkom Akademie ist [anerkannter Bildungsträger in Baden-Württemberg](#) und [Nordrhein-Westfalen](#). Teilnehmende haben im Rahmen des Bildungszeitgesetzes die Möglichkeit, Bildungsurlaub bzw. eine Bildungsfreistellung zu beantragen. Auf Anfrage erstellen wir auch Anträge auf Anerkennung unserer Veranstaltungen in anderen Bundesländern.
- Wir erklären ausdrücklich, dass beim Bitkom – Unterzeichner der Charta der Vielfalt – jede Person, unabhängig von Geschlecht, Nationalität, ethnischer Herkunft, Religion oder Weltanschauung, Behinderung, Alter, sexueller Orientierung und Identität willkommen ist.

Seminarprogramm

Cyber Resilience Act in der Anwendung

Tag
1

Grundlagen des Cyber Resilience Act (CRA)

- Hintergrund der Gesetzgebung
- Geltungsbereich und Zielsetzung, Wichtige Akteure und Verantwortlichkeiten
- Kernelemente des CRA: Überblick über die grundlegenden Anforderungen

Rechtliche Anforderungen und Compliance-Pflichten

- Durchführung von Risikoanalysen, Erstellung technischer Dokumentation und EU-Konformitätserklärung für Produkte
- Cybersecurity-Anforderungen umsetzen: Welche organisatorischen Maßnahmen müssen ergriffen werden, um »angemessene« Sicherheit zu gewährleisten?
- CE-Kennzeichnung und Konformitätsverfahren, Umgang mit Schwachstellen
- Konsequenzen bei Nichteinhaltung: Überblick über die Durchsetzung und mögliche Sanktionen bei Verstößen gegen den CRA

Best Practices zur CRA-Umsetzung

- Integration in betriebliche Prozesse: Wie lässt sich der CRA in bestehende Unternehmensprozesse integrieren?
- Abgleich mit bestehenden Standards: Zusammenhänge des CRA mit anderen Regelwerken und Normen
- Praktische Ressourcen: Hinweise auf Leitfäden, Checklisten und Unterstützungsangebote

Erarbeitung eines Maßnahmenplans

- Fahrplan und Maßnahmen entwickeln, Priorisierung und Zeitplanung
- Erfahrungsaustausch der Teilnehmenden

Ihre Referentin



Sophie Powierski

Compliance Beraterin
Bredex GmbH

Nach ihrem Masterabschluss in Good Governance – Rechtsgestaltung (LL.M.) an der Universität Rostock, arbeitete Sophie Powierski zunächst als Trainee im Bereich Datenschutz und Informationssicherheit bei der Bredex GmbH und ist dort nun als Compliance Beraterin beschäftigt.

Shortfacts



Termine, Preise und Veranstaltungsorte

Bitte entnehmen Sie aktuelle Informationen hierzu Website der [Bitkom Akademie](#).

Kontaktieren Sie uns – wir beraten Sie gern.

Bitkom Akademie | Albrechtstraße 10 | 10117 Berlin
T 030 27576-540 | info@bitkom-akademie.de
Weitere Seminare finden Sie unter www.bitkom-akademie.de

bitkom
akademie