Cyber Resilience Act (CRA)
Cybersicherheit für digitale Produkte

Mehr Cybersicherheit für Produkte mit digitalen Elementen

Immer mehr Produkte enthalten digitale Komponenten, um den steigenden Anforderungen an Konnektivität und Funktionalität gerecht zu werden. Doch das Cybersicherheitsniveau ist oft unzureichend und Anwender können schwer erkennen, welche Produkte tatsächlich sicher sind.

Das EU-Gesetz über Cyberresilienz, der **Cyber Resilience Act (CRA)**, zielt darauf ab, Verbraucher und Unternehmen zu schützen, die Produkte oder Software mit einer digitalen Komponente kaufen oder verwenden. Das Gesetz verpflichtet Hersteller dazu, umfangreiche Cybersicherheitsmaßnahmen über den gesamten Produktlebenszyklus hinweg umzusetzen – von der Entwicklung über die Bereitstellung bis hin zu Updates und dem Umgang mit Schwachstellen.

Der CRA gilt für Produkte, Software und Hardware mit digitalen Elementen und betrifft damit zahlreiche Branchen – von vernetzten Geräten und Embedded-Systemen über Softwareprodukte und Cloud-Dienste bis hin zu branchenspezifischen Lösungen.

Der CRA trat am 11. Dezember 2024 in Kraft und wird schrittweise umgesetzt. Bis Ende 2027 müssen alle neuen Produkte die CRA-Vorgaben erfüllen.

Unsere Security Engineering Leistungen

Workshop: Einführung in das EU-Gesetz über Cyberresilienz

- Cybersicherheits-Risiken für Hersteller
- Das Gesetz zur Cyberresilienz verstehen
- Daraus resultierende Anforderungen an die Cybersicherheit von Unternehmen und ihren Prozessen
- Daraus resultierende Anforderungen an die Cybersicherheit von Produkten mit digitalen Elementen

Bestandsaufnahme und CRA-Gap-Analyse

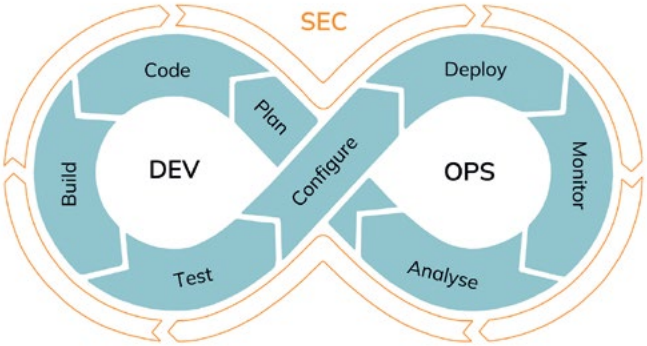
- Analyse ausgewählter Produkte des Kundenportfolios
- Vertraut machen mit dem zu analysierenden Produkt und Identifizierung der relevanten Anforderungen des Gesetzes über Cyberresilienz
- Analyse des Ist-Zustandes mit Bezug auf den CRA
- Identifizierung von Lücken zum CRA
- Erstellung eines Aktionsplans

Bedrohungsanalyse und Risikobewertung (TARA)

- Analyse ausgewählter Produkte des Kundenportfolios
- Workshop zur Produktkonsolidierung und Identifizierung von Produkt-Assets
- Bedrohungsanalyse und Risikobewertung (TARA) durch erfahrene Security Consultants
- Workshop zur Risikominderung
- Ausführlicher TARA-Bericht

Weitere Leistungen im Secure Development Lifecycle (SDL):

- Sicherheitskonzeption und Sicherheitsarchitektur
- Sichere Produktentwicklung
- Härtung von Software- und Systemkomponenten
- Beratung zu Security Engineering Werkzeugen
- Testen der Sicherheitsfunktionen
- Schwachstellen- und Pentesting
- Unterstützung bei der Konformitätsbewertung



Cybersicherheit von Anfang an

achelos unterstützt Sie professionell und effizient bei der CRA-Compliance Ihrer Produkte. Unsere Security Engineers begleiten Sie während der Entwicklung und sorgen für integrierte Cybersicherheit von Anfang an – praxisnah, normorientiert und regulatorisch fundiert.

Machen Sie Ihre Entwicklung zukunftssicher – sprechen Sie uns an!

achelos GmbH Paderborn T +49 5251 14212-0 info@achelos.de www.achelos.de