OVSoftware

Guide

Der EU Cyber Resilience Act einfach erklärt & wie du ihn erfüllst

8 konkrete Handlungsempfehlungen für dein Unternehmen

Der EU Cyber Resilience Act (CRA)

Der Cyber Resilience Act (CRA) der Europäischen Union ist Ende 2024 in Kraft getreten. Das Gesetz ist die Reaktion der Europäischen Union auf die stetig wachsende Cyberkriminalität. Der CRA ist der Versuch, das Cyberrisiko von Produkten zu minimieren.

Was das genau bedeutet, ob es dein Unternehmen betrifft und welche Auswirkungen der CRA konkret hat, erfährst du in diesem Leitfaden von OVSoftware.

Fangen wir also mit der relevantesten Frage für dich an:

Betrifft der CRA dein Unternehmen?

Dein Unternehmen kann nur unter den CRA fallen, falls du entweder Hersteller, Importeur oder Händler von Hard- oder Softwareprodukten bist, die Daten austauschen oder dazu fähig sind. Falls das nicht der Fall ist, ergibt sich aus der Einführung des CRA kein Handlungsbedarf für dich.

Wenn dein Unternehmen aber in eine der Kategorien fällt, kommt es darauf an, welche Produkte du herstellst, importierst oder womit du handelst. Das Gesetz unterscheidet insgesamt 4 verschiedene Produktkategorien nach ihrer Relevanz. (Die Liste ist aufsteigend. Je später dein Produkt, desto strenger die Auflagen):

1.Standardprodukte

Produkte, die keinerlei „cybersicherheitsrelevante“ Aufgaben erfüllen. Das können Softwarekomponenten zur Bild- oder Textverarbeitung sein. Oder z.B. ein Staubsaugerroboter, der für Updates einen Internetzugang besitzt. Ähnlich verhält es sich mit einer Spielkonsole.

2. Kritische Produkte der Klasse I

Produkte, die als kritisch für die Cybersicherheit gelten, weil sie wichtige Aufgaben erfüllen. Dazu gehören Passwortmanager, VPNs, Antivirensoftware oder bestimmte Netzwerkkomponenten.

3. Kritische Produkte der Klasse II

Produkte, die als kritisch für die Cybersicherheit gelten, weil sie wichtige Aufgaben erfüllen und unentdeckte Sicherheitslücken weitreichende Folgen auf umliegende Systeme haben.
Beispiele sind Betriebssysteme, industrielle Firewalls und Sicherheitslösungen, Router und Modems für die Industrie oder Chipkarten und Chipkartenlesegeräte.

4. Hochkritische Produkte

Zu guter Letzt legt die EU besonderen Wert auf den Schutz von kritischer Infrastruktur (bspw. den Energiesektor) und hat hier bestimmte Software und Hardware definiert, die als besonders schützenswert gilt.
Ein Beispiel: Smart-Metering-Gateways, die Energieverbrauchsdaten in Echtzeit messen und versenden.

Die genaue Liste kannst du hier im Anhang zum CRA nachschlagen.

Welchen Sinn verfolgt der CRA eigentlich?

Der Cyber Resilience Act soll sowohl Unternehmen als auch Einwohner innerhalb der EU effektiver vor Cyberbedrohungen schützen. Der Fokus liegt aber vor allem auf Unternehmen.

Ziel ist es, alle „digitalen Produkte" per Gesetz sicherer zu machen. Wie du an den angeführten Beispielen erkennst, kann das sowohl Hardware als auch Software betreffen.

Genauer geht es darum, Schwachstellen zu identifizieren und zu beheben. Außerdem verpflichtet das Gesetz standardmäßig zu einer Sicherheitsgarantie, die mehrere Jahre gültig sein soll, wobei die exakte Anzahl der Jahre vom Produkt abhängt.

Aber auch die Aufklärung über deine Sicherheitsvorkehrungen und die einheitliche Kennzeichnung deiner Produkte spielen eine Rolle.

Was sich aus diesen Ansprüchen für dein Unternehmen ableitet, erfährst du jetzt.

Welche Anforderungen stellt der CRA konkret an dein Unternehmen?

Je nachdem, ob du Hersteller, Importeur oder Händler von digitalen Produkten bist, unterscheiden sich die gesetzlichen Forderungen an dein Unternehmen.

Was gilt für dich, wenn du Hersteller bist?

Als Hersteller musst du jedes deiner Produkte einer Konformitätsprüfung unterziehen. Das bedeutet, dass du die Erfüllung der festgelegten Cybersicherheitsanforderungen des CRA nachweisen musst. Das Ergebnis ist in einer Konformitätserklärung festzuhalten.

Weitere Herstellerpflichten umfassen:

- Eine unauslöschliche CE-Kennzeichnung, die am Produkt oder der Verpackung angebracht ist und sich auch in der Konformitätserklärung wiederfindet.
- Die Erstellung einer Gebrauchsanleitung, die vor allem die richtige Installation, Wartung und Nutzung deines Produktes sicherstellt.
- Die fortlaufende Dokumentation technischer Details, damit du nachweisen kannst, dass dein Produkt jederzeit den Ansprüchen der CRA genügt.
- Regelmäßige Sicherheitsupdates deiner Software- oder Hardwarelösung, bis du das Produkt vom Markt nimmst oder die Garantie von maximal 5 Jahren verfällt.
- Das Melden von Sicherheitslücken und -vorfällen, die deine digitalen Produkte betreffen.

Außerdem impliziert das Gesetz, dass du jedes digitale Produkt nach dem Leitsatz „Security by Design” entwickelst. Dazu mehr bei deinen konkreten Handlungsempfehlungen.

Was gilt für dich, wenn du Importeur oder Händler bist?

Als Importeur oder Händler von digitalen Produkten bist du dazu verpflichtet, zu überprüfen, ob der Hersteller seine Pflichten erfüllt hat.

Gibt es eine Konformitätsbeurteilung, CE-Kennzeichnungen und Gebrauchsanleitung? Alle technischen Details müssen stimmen. Händler müssen auch noch die Kontaktdaten des Importeurs abfragen und aufbewahren.

Wie sorgst du dafür, dass dein Unternehmen die Anforderungen des CRA problemlos erfüllt?

Bestimmt hast du jetzt schon eine Vorstellung, wo dein Unternehmen im CRA einzuordnen ist und welche Verpflichtungen deswegen auf dich zukommen.

Viel dringender ist aber die Frage, welche Maßnahmen du konkret umsetzen kannst, um das Gesetz problemlos zu erfüllen. Diese Handlungsempfehlungen ermöglichen dir, dein digitales Produkt in Einklang mit der neuen Rechtsverordnung zu bringen.

Deine 8 Handlungsempfehlungen

1 Nutze einen automatisierten Schwachstellenscanner

Der Gesetzestext legt besonderen Wert darauf, dass „bekannte und ausnutzbare Schwachstellen“ in deinen Produkten vermieden werden. Aus technischer Sicht darf es also keine Bestandteile geben, die bei Cyberattacken bereits als Einfallstor gedient haben.

Oft betrifft das vor allem Drittsoftware. Deswegen bietet es sich an, eine Lösung zu nutzen, um alle Bestandteile deines Produktes kontinuierlich auf Schwachstellen zu überprüfen. Das spart dir viel Zeit, weil du die mühsame, manuelle Überprüfung ersetzt.

2 Fertige eine umfassende Software-Stückliste an

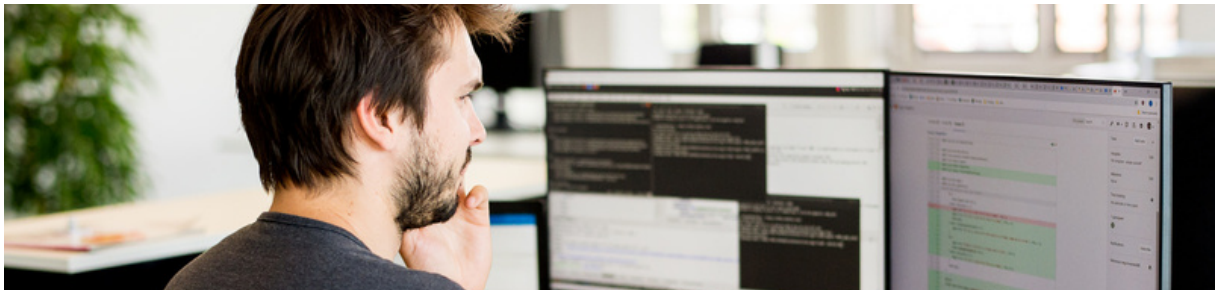
Es gibt kaum Produkte, die ausschließlich auf eigenem Code basieren. Sicher hast auch du an einer oder mehreren Stellen eine Bibliothek genutzt oder andere Abhängigkeiten erzeugt. Bisher war das selten ein Problem, doch nun brauchst du eine nachweisliche Übersicht.

Deswegen empfehlen wir dir, eine umfassende Software-Stückliste (SBOM) anzufertigen. Im Idealfall werden alle direkten und indirekten Abhängigkeiten sofort erkenntlich. So fällt es dir leicht zu beurteilen, ob du eine kritische Sicherheitslücke hast (bspw. Log4Shell).

3 Sorge für kontinuierliche Updates deiner Produkte

Sobald der CRA offiziell zu geltendem Recht wird, bist du verpflichtet, die Sicherheit deiner digitalen Produkte zu garantieren. Ohne kontinuierliche Updates ist das unmöglich.

Achte darauf, dass du die gefundenen Schwachstellen deiner Scans und bereits bekannte Schwachstellen von Drittsoftware mit Updates zeitnah behebst. Indem du deine Produkte immer auf dem neuesten Stand hältst, vermeidest du potenzielle Strafzahlungen effektiv.



4 Setze bei deiner Softwarearchitektur auf Best Practices

Jederzeit Anpassungen an deiner Software vornehmen zu können, wird zukünftig eine bedeutende Rolle spielen, damit du Updates einfach und kostengünstig umsetzen kannst.

Deswegen lohnt es sich für dich, wenn du das bereits in der Konzeptionsphase bei neuen Projekten im Hinterkopf behältst. Nutze Best Practices und automatisierte Softwaretests, um sicherzustellen, dass deine Softwarearchitektur zukünftig leicht zu warten ist.

5 Verbessere die Sicherheit deiner Software durch „Security by Design“

Der CRA legt seinen Hauptfokus auf die Sicherheit von digitalen Produkten. Du kannst dir also einige Arbeit sparen, wenn du bereits bei der Konzeption und während der Entwicklung auf regelmäßige Sicherheitschecks setzt.

„Security by Design” umfasst auch, die Konfigurationen möglichst sicherzumachen, indem du die Sicherheitsvorkehrungen passgenau an den späteren Nutzungszweck anpasst. Zugriffsrechte, die sichere Verschlüsselung von Daten und Audit Logs sind weitere Grundprinzipien, um Schwachstellen proaktiv zu vermeiden.

6 Dokumentiere deinen gesamten Entwicklungsprozess

Die technische Dokumentation ist eine der Pflichten, die sich für Hersteller aus dem CRA ergibt. Aber die Dokumentation deines Entwicklungsprozesses lohnt sich unabhängig davon immer für deine Software-Projekte.

Halte am besten den Zweck, verwendete Technologien, Qualitäts-anforderungen und -entscheidungen fest, um jederzeit deinen Entwicklungsprozess nachvollziehen zu können. So findest du nicht nur leichter Fehlerursachen, sondern kannst auch die Sicherheit deiner Lösungen gezielt überprüfen und – wenn nötig – verbessern.

Eine gängige Methode stellt bspw. das arc42 Template dar, um die Architektur deiner Software einfach und nachvollziehbar zu doku-mentieren.

7 Überprüfe am besten auch bestehende Systeme, für die du verantwortlich bist

Bestehende digitale Produkte fallen nach der Übergangsfrist auch unter den CRA, falls wesentliche Updates vorgesehen sind. Wenn du frühzeitig damit beginnst, den Quellcode, die Software-Architektur und Drittbibliotheken zu überprüfen, hast du später weniger Arbeit.

Auch hier gilt: Die technische Dokumentation wird im Zweifelsfall nochmal wichtig.

8 Definiere frühzeitig einen passenden Prozess

Jetzt ist noch viel Zeit, um einen Prozess auszuarbeiten, der später sicherstellt, dass alle Anforderungen des CRA einfach erfüllt werden. Du profitierst also, wenn du dir frühzeitig Gedanken machst, wie du Sicherheitslücken findest, meldest und zeitnah beseitigst.

Welche Konsequenzen drohen deinem Unternehmen, wenn du den CRA nicht erfüllst?

Wenn dein Unternehmen den Anforderungen und Pflichten des CRA nicht gerecht wird, drohen dir Bußgelder in Höhe von bis zu 15 Millionen Euro oder 2,5 % des jährlichen Umsatzes.

Das empfindlich hohe Strafmaß beweist, dass es die EU mit der Verbesserung von Cybersicherheit ernst meint und sich eine rege Teilnahme von allen Herstellern erhofft.

Wie viel Zeit bleibt dir noch zur straffreien Erfüllung der Auflagen?

Die EU sieht – nach Inkrafttreten – eine Schonfrist von 12 Monaten vor, um alle Anforderungen als Hersteller zu erfüllen. Und da der CRA noch dieses Jahr umgesetzt werden soll, könnte es nächstes Jahr zu dieser Zeit schon knapp werden.

Wie kannst du sicherstellen, dass deine digitalen Produkte rechtzeitig alle Anforderungen des CRA erfüllen?

Wenn du jetzt beginnst, diese praxisnahen Handlungsempfehlungen umzusetzen, solltest du es schaffen, allen deinen Herstellerpflichten gerecht zu werden.

Falls du noch Fragen zum CRA hast oder dich bei dessen Erfüllung unterstützen lassen möchtest, schreibe mir gerne eine Nachricht auf LinkedIn.

Dominik Antulov

Senior Account Manager
OVSoftware GmbH
+49 (0)251 609 700 13
+49 (0)1578 2201 522
dominik.antulov@ovsoftware.de
linkedin.com/in/dominikantulov

OVSoftware GmbH, Hafenweg 46, 48155 Münster, 0251 609 700 0

OVSoftware