Verbandsnews

Mythbusting CRA: Nicht alle Gerüchte über den Cyber Resilience Act sind wahr

Nachdem der Gesetzestext für den Cyber Resilience Act (CRA) beschlossen wurde, setzen sich immer mehr Unternehmen damit auseinander, was da jetzt genau auf sie zukommt und welche Anforderungen sie erfüllen müssen. Die Uhr tickt: Ende 2027 müssen alle Unternehmen die Anforderungen des CRA vollständig erfüllen, einige Anforderungen allerdings schon ab Mitte 2026.

Der CRA führt einige ganz neue Regelungen und Konzepte ein, die es so bisher noch nie gab. Das führt zu diversen Missverständnissen und es sind etliche Mythen und Gerüchte rund um den CRA im Umlauf. Diese führen zum Teil stark in die Irre oder machen den Betroffenen unnötigerweise Angst. Deswegen wollen wir hier einige der Mythen, die im Umlauf sind und die uns immer wieder begegnen, vorstellen und widerlegen. Damit können wir hoffentlich einigen Betroffenen ein paar Unsicherheiten nehmen.

Wer selbst tiefer in die einzelnen Artikel des CRA eintauchen möchte, auf die hier auch immer wieder verwiesen wird, kann sich gerne die von unserer Task Force CRA erarbeitete „Requirements Analyse“ (als .xlsx oder als .odt) herunterladen. Hier sind alle Artikel und Paragrafen des CRA auf Deutsch und Englisch nebeneinander gestellt. Zusätzlich gibt es in dem Tabellendokument die Möglichkeit, den gesamten Text des CRA nach bestimmten Rollen, Akteuren oder Anforderungen zu filtern.

Noch ein Disclaimer: Unsere Einschätzung zu den verschiedenen Mythen und der Frage, wie der CRA-Text zu interpretieren ist, stellt keine Rechtsberatung dar.

Mythos 1: In der Freizeit entwickelte Software fällt auch unter den CRA.

Nein, der CRA stellt unter anderem Anforderungen an Verwalter quelloffener Software ("open source software stewards", Art. 24) und Hersteller von Produkten mit digitalen Inhalten ("manufacturer", Art. 13 & 14). Diese zwei Kategorien sind am nächsten dran an juristischen oder natürlichen Personen, die in ihrer Freizeit Software entwickeln, und die den CRA befolgen müssen. Ein Freizeit-Entwickler und demnach seine Software fallen nur dann (!) unter den CRA, wenn der Entwickler mindestens einer der Definitionen dieser beiden Kategorien entspricht.

Open Source Software Stewards:

Um als Verwalter quelloffener Software ("open source software steward") zu zählen, muss folgendes erfüllt sein (Art. 3 Nr. 14):

- Es muss sich um eine juristische Person handeln.
- Es darf sich nicht um einen Hersteller handeln.
- Die juristische Person verfolgt die spezifische Zielsetzung oder den Zweck, Open Source Software zu entwickeln.
- Die entwickelte Open Source Software ist für kommerzielle Tätigkeiten bestimmt.
- Die juristische Person verfolgt die nachhaltige und systematische Unterstützung der Open Source Software und stellt die Brauchbarkeit dieser Produkte sicher.

Ob es sich bei einer juristischen Person um eine ausschließlich juristische Person handeln muss oder nicht, ist unklar. Da aber der CRA mehrmals zwischen juristischen Personen und natürlichen Personen unterscheidet (Art. 3 Nr. 13, 15, 16, 17, 18), kann hier die Annahme getroffen werden, dass es sich hier um eine ausschließlich juristische Person handeln muss.

Manufacturer:

Um im Sinne des CRA als Herstellerzu gelten, muss u.a. folgendes erfüllt sein (Art. 3 Nr. 13):

- Eine natürliche oder juristische Person, die ein Produkt unter dem Namen oder der Marke des potenziellen Herstellers vermarktet.
- Das Produkt wird im Rahmen einer Geschäftstätigkeit („in the course of a commercial activity“) vertrieben oder verwendet (Art. 3 Nr. 22).

Dementsprechend gilt: Solange ein Hobby-Entwickler seine Software nicht im Rahmen eines Vereins oder einer Stiftung mit dem Ziel der Bereitstellung von Software für kommerzielle Zwecke oder im Rahmen einer Geschäftstätigkeit veröffentlicht, ist er nicht vom CRA betroffen.

Mythos 2: Kleine und mittlere Unternehmen (KMUs) müssen den CRA nicht befolgen.

Der CRA soll langfristig gewährleisten, dass Produkte mit digitalen Elementen auch wirklich sicher sind. Dementsprechend ist der CRA allgemeingültig und auch kleine und mittlere Unternehmen (KMUs) müssen den CRA befolgen. Aber der CRA will für KMUs ausgewählte Erleichterungen schaffen, dazu gehört u.a.:

- Die Unterstützung durch einen Helpdesk zu Meldepflichten (Art. 17 Abs. 6).
- Ein Ermessensspielraum bei Bußen und Gebühren für KMUs (Art. 64 Abs. 5 c und Art. 32 Abs. 6).

- Eine Verhältnismäßigkeit bei den Konformitätsbewertungen sowohl mit Blick auf den Umfang der Anforderungen (Art. 47 Abs. 2) als auch mit Blick auf die Gebühren des Konformitätsbewertungsverfahrens für KMUs (Art. 39 Abs. 12).
- Eine vereinfachte Version der benötigten Technischen Dokumentation für Klein- und Kleinstunternehmen (Art. 33 Abs. 5).
- Potenzielle finanzielle Unterstützung im Rahmen bestehender EU-Programme (Art. 33 Abs. 4).
- Leitlinien in Bezug auf die Durchführung der Verordnungen (Art. 26 Abs. 1 und Art. 33 Abs. 3).
- Gegebenenfalls Schulungen als Maßnahme der Mitgliedsstaaten für Klein- und Kleinstunternehmen (Art. 33 Abs. 1 a).
- Gegebenenfalls spezielle Kommunikationskanäle für Klein- und Kleinstunternehmen und lokale Behörden zur Durchführungshilfe und für Rückfragen (Art. 33 Abs. 1 b).
- Gegebenenfalls Unterstützung von Prüf- und Konformitätsbewertungstätigkeiten (Art. 33 Abs. 1 c).
- Gegebenenfalls Zugang zu kontrollierten Prüfumgebungen für innovative Produkte für Klein- und Kleinstunternehmen sowie Start-ups (Art. 33 Abs. 2).

Der Grund, warum bei einigen Punkten noch "gegebenenfalls" steht, ist der, dass derzeit noch etliche konkrete Umsetzungsanforderungen auf EU-Ebene ausgearbeitet werden. Das gleiche gilt auch für Unterstützungsprogramme, die die EU anbieten will. Hier wird es hoffentlich in den kommenden Jahren nach und nach immer konkretere Informationen darüber geben, welche Unterstützung KMUs in Anspruch nehmen können.

Mythos 3: Als Hersteller darf/kann ich keine Open Source Software mehr einsetzen.

Man darf nach wie vor Open Source Software einsetzen, es wird von den Unternehmen allerdings eine gewisse Sorgfalt abverlangt: "Manufacturers shall exercise due diligence when integrating components from third parties". Hier liegt es am Hersteller, dafür zu sorgen, dass von Dritten bezogene Komponenten (auch Open-Source-Komponenten) die Cybersicherheit des Produkts nicht beeinträchtigen (Art. 13 Abs. 5). In Bezug auf die Sicherheitsanforderungen dieser Komponenten sollen auch freiwillige Programme zur Bescheinigung der Sicherheit kommen, welche diese Sorgfaltspflicht erleichtern sollen (Art. 25).

Diese Anforderung aus dem CRA zwingt also die Hersteller dazu, sich mit ihrer Software-Lieferkette auseinander zu setzen. Denn am Ende müssen sie die Verantwortung für das fertige Produkt übernehmen, das sie auf den Markt bringen. Darin steckt auch eine Chance, denn heutzutage integrieren viele auch große und umsatzstarke Unternehmen gerne kostenlos verfügbare Open-Source-Komponenten, investieren aber selber nichts in die Pflege und Sicherheit dieser Basiskomponenten, von deren Verwendung sie so stark

profitieren. Der CRA führt hier dazu, dass entlang der Lieferkette mehr Akteure Verantwortung übernehmen und sich auch um die Sicherheit der verwendeten Komponenten kümmern müssen.

Mythos 4: Schwachstellen müssen innerhalb von 7 Tagen **behoben** sein.

Wir konnten im CRA keine Erwähnung einer 7-Tage-Frist für das Beheben von Schwachstellen finden. Was wir aber finden konnten, sind Meldungen über Schwachstellen, die ab und bis zu bestimmten Zeitpunkten verlangt sind, sowie die in Anhang I Teil 2 Nr. 8 beschriebene „Unverzüglichkeit" der Bereitstellung des Sicherheitsupdates zu einer Schwachstelle. Im Kontext des deutschen Rechts bedeutet ‚unverzüglich' ‚ohne schuldhaftes Zögern', was wir als die sofortige Bearbeitung der Schwachstelle interpretieren, wobei der dafür erforderliche Zeitraum egal ist. Die Melde-Deadlines variieren je nachdem, ob es sich um eine Schwachstelle handelt oder um einen Sicherheitsvorfall beim Hersteller.

Die Meldefristen für Meldungen an die zuständige Marktaufsichtsbehörde sind:

- Unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme einer aktiv ausgenutzten Schwachstelle oder eines Sicherheitsvorfalls des Herstellers muss eine Schnellmeldung eines Vorfalls oder einer Sicherheitslücke gemacht werden.
- Unverzüglich, in jedem Fall aber innerhalb von 72 Stunden nach Kenntnisnahme einer aktiv ausgenutzten Schwachstelle oder eines Sicherheitsvorfalls des Herstellers müssen alle bis zu dem Zeitpunkt verfügbaren Informationen übermittelt werden.
- Spätestens 14 Tage nachdem eine Korrektur oder Risikominderungsmaßnahme für eine aktiv ausgenutzte Schwachstelle zur Verfügung steht, muss ein abschließender Bericht vorgelegt werden.
- Einen Monat nach Übermittlung der 72-Stunden-Meldung bei einem Sicherheitsvorfall des Herstellers muss ein abschließender Bericht vorgelegt werden.

Die benötigten Informationen, die zu den jeweiligen Zeitpunkten übermittelt werden müssen, kann man im Artikel 14 des CRA nachlesen.

Mythos 5: Die technische Dokumentation MUSS veröffentlicht werden.

Unserer Recherche zufolge muss eine technische Dokumentation nur in bestimmten Fällen veröffentlicht werden, die in Art. 32 Abs. 5 ausgeführt werden. Im Normalfall liegt die technische Dokumentation aber beim Hersteller und wird bei Bedarf gepflegt.

Die technische Dokumentation muss auf Anfrage der Marktüberwachungsbehörden ausgehändigt werden (Art. 13 Abs. 13), sowie bei manchen Konformitätsbewertungsverfahren (Art. 53), und an einen Einführer/Importeur, falls es ein Produkt ist, welches außerhalb des EU-Marktes hergestellt und in die EU importiert wird (Art. 19 Abs. 2).

Mythos 6: Ich muss eine Software Bill of Materials (SBOM) erstellen und veröffentlichen.

Erstellt werden muss eine SBOM auf jeden Fall (Anhang I Teil II Nr. 1) und diese SBOM muss in die technische Dokumentation eingefügt werden (Anhang VII Nr. 2b/8). Von einer obligatorischen Veröffentlichung der SBOM ist im CRA allerdings nicht die Rede. Eine SBOM kann freiwillig veröffentlicht werden (Anhang II Nr. 9), es besteht allerdings kein genereller Zwang.

Da die SBOM Teil der technischen Dokumentation ist, muss sie auf Anfrage an die Marktüberwachungsbehörden (Art. 13 Abs. 13), bei manchen Konformitätsbewertungsverfahren (Art. 53) sowie an einen Einführer/Importeur in die EU ausgehändigt werden (Art. 19 Abs. 2).

Mythos 7: Software Bills of Material (SBOMs) sind nicht von Bedeutung.

SBOMs bzw. Softwarestücklisten werden im CRA erwähnt und als notwendiges Mittel zur Ermittlung und Dokumentation von Schwachstellen und Komponenten genannt (Annex I Teil II Nr. 1). Unabhängig vom Zwang der Erstellung ist die SBOM ein zentrales Werkzeug, um mit den darin enthaltenen Daten die Erfüllung anderer CRA-Anforderungen zu ermöglichen.

Mythos 8: Der CRA fordert "Security by Design".

"Security by Design" kommt als eigener Begriff im Gesetzestext nicht direkt vor. Der CRA verlangt aber die Auseinandersetzung mit Sicherheitsfragen schon beim Design eines Produkts mit digitalen Elementen, sowie beim Entwicklungs- und Herstellungsprozess (Anhang I Teil 1 Nr. 1). Es soll also schon während des Designs/der Architektur auf die Sicherheit geachtet werden. Was der CRA in der englischsprachigen Fassung allerdings tatsächlich spezifisch nennt, ist eine "secure by default" Konfiguration (Anhang I Teil 1 Nr. 2b).

Es handelt sich hier also eher um eine sprachliche Unschärfe oder Ungenauigkeit. Im CRA werden zwar nicht alle der gängigen Anforderungen, die im Zusammenhang mit "security by design" üblich sind, gefordert, gleichzeitig will der CRA eben darauf hinwirken, dass IT-Sicherheit bereits beim Design-Prozess berücksichtigt wird.

Mythos 9: Der CRA besitzt keine Ausnahmen.

Die Ausnahmen des CRA sind alle in Artikel 2 des Gesetzestextes hinterlegt. Diese sind nicht ganz einfach zu lesende Verweise auf verschiedene EU-Richtlinien und -Verordnungen.

Produkte, die unter die folgenden Richtlinien und Verordnungen fallen, müssen den CRA nicht befolgen, da sie bereits unter andere (ggf. sogar strengere) sektorale Regelungen fallen:

- Medizinprodukte (Art. 2 Abs. 2 a) nach EU-Verordnung 2017/745.
- In-vitro-Diagnostika (Art. 2 Abs. 2 b) nach EU-Verordnung 2017/746.

- Autoindustrie („automotive“) (Art. 2 Abs. 2 c) nach EU-Verordnung 2019/2144.
- Nach Luftfahrtsverordnung 2018/1139 zertifizierte Produkte (Art. 2 Abs. 3).
- Schifffahrtsausrüstung nach Richtlinie 2014/90/EU (Art. 2 Abs. 4).

Wichtig hierbei: Die Ausnahme gilt nur, wenn ein Produkt auch wirklich in den Anwendungsbereich der entsprechenden Richtline oder Verordnung fällt. Dies ist im Zweifelsfall genau zu prüfen.

Bitte außerdem beachten: Bei Produkten, die aufgrund ihrer Anwendung gleichzeitig in eine der oben genannten Regelungen fallen und das Potential besitzen, außerhalb dieser Regelungen genutzt zu werden, ist bisher noch nicht abschließend geklärt, inwieweit diese auch zusätzlich unter den CRA fallen.