Security Cyber Lounge
CRA & OWASP SAMM

Fragen & Antworten

Autor SBA Research gGmbH

Datum 28.07.2025

Kontakt Stefan Jakoubi (sjakoubi@sba-research.org)

Gerald Sendera (gsendera@sba-research.org)

Mathias Tausig (mtausig@sba-research.org)

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie

Bundesministerium Arbeit und Wirtschaft

FFG Forschung wirkt.

wirtschaftsagentur wien

Für die Stadt Wien

FWF Österreichischer Wissenschaftsfonds

netidee FÖRDERUNGEN

Fragen & Antworten

⚠ Diese Informationen sind keine Rechtsberatung und können eine solche auch nicht ersetzen!

 # Ist der CRA auch auf Softwareprodukte anwendbar, wenn die Software nur unternehmens- bzw. konzernintern genutzt wird?

Siehe Antwort auf die folgende Frage zu „Eigenbedarf".

 # Gilt das auch für Software, die nur im Eigenbedarf verwendet wird?

Das entscheidende Kriterium ist: „Wird die Software auf dem Markt kommerziell angeboten?" Wenn ja, dann fällt sie vermutlich unter den CRA. Individualsoftware für Kund:innen oder auch Eigenentwicklungen, die man nur selbst verwendet, sind nicht davon betroffen. Die Erfüllung der Anforderungen macht aber wahrscheinlich trotzdem Sinn.

 # Wird das CE-Kennzeichen zur Unterscheidung von alten CE-Kennzeichnungen Merkmale für CRA haben? Und kann ich die Klasse I/II/kritisch am Produkt erkennen?

Nach jetzigem Stand; nein bzw. noch nicht. Das CE-Kennzeichen entspricht den derzeit noch geltenden Standards für dessen Anbringung, vgl. dazu auch Hinweise und Verweise im „Blue Guide" („Bekanntmachung der Kommission: Leitfaden für die Umsetzung der Produktvorschriften der EU 2022"). Artikel 30 der VO beschreibt Details über die Anbringung und Gestaltung des Kennzeichens. So KANN zukünftig nach Abs. 3 eine zusätzliche Kennzeichnung über ein besonderes Cybersicherheitsrisiko angebracht werden (aber dann eben „zusätzlich" zum CE-Kennzeichen). Das allerdings nur, sofern es dazu einen delegierten Rechtsakt geben wird. Und das wiederum müsste nach Abs. 6 erst festgelegt werden.

 # Medizinprodukte sind ausgenommen; ist rechtlich auch hier etwas im Kommen, das sicherheitstechnisch nachgezogen wird? Haben andere Länder schon schärfere Sicherheitsmaßnahmen für Medizinprodukte?

Die erste Frage können wir aus heutiger Sicht nicht beantworten. Es gibt bereits einige nationale und internationale Standards, die Cybersicherheit von Medizinprodukten adressieren.

Zur zweiten Frage: Inwieweit es international derzeit (noch) strengere sektorale Gesetzgebung gibt, ist uns nicht bekannt.

 # Welche FOSS-Projekte und -Bibliotheken werden sich überhaupt dem CRA beugen, da diese meist in den USA angesiedelt sind? Ich unterstelle jetzt bei meiner Frage dem Hersteller eine Gewinnabsicht, sodass die SW unter den CRA fällt.

Kommerzielle amerikanische OSS Anbieter wie Redhat oder Gitlab müssen sich daran halten, wenn sie eine Zulassung zum Markt wollen. Wie das dann konkret exekutiert wird, ist eine andere Frage.

Generell muss aber gesagt werden, dass die Umsetzung der Anforderungen bei physischen Produkten tendenziell schwieriger ist als bei reiner Software.

 # Unterliegen Softwareprodukte dem CRA, die von der öffentlichen Verwaltung entwickelt wurden und weiten Teile der Bevölkerung (Steuerzahler, Versicherte, Dienstgeber, Gesundheitsdienstleister udgl.) zur Verfügung stehen? (zB. Digitales Amt)

Nach heutigem Stand: nein.

Siehe dazu Erw.Gr. 16 *„Produkte mit digitalen Elementen, die im Rahmen der Erbringung einer Dienstleistung bereitgestellt werden, für die eine Gebühr ausschließlich zur Deckung der tatsächlichen Kosten erhoben wird, die in unmittelbarem Zusammenhang mit dem Betrieb dieses Dienstes stehen, wie dies bei bestimmten Produkten mit digitalen Elementen der Fall sein kann, die von Einrichtungen der öffentlichen Verwaltung bereitgestellt werden, sollten nicht allein aus diesen Gründen als Bestandteil einer Geschäftstätigkeit im Sinne dieser Verordnung angesehen werden. Darüber hinaus sollten Produkte mit digitalen Elementen, die von einer öffentlichen Verwaltungseinrichtung ausschließlich für ihren Eigenbedarf entwickelt oder geändert werden, nicht als auf dem Markt bereitgestellt im Sinne dieser Verordnung gelten."*

 # Sind Web-Self-Care-Anwendungen auch betroffen?

Wenn sie als Medizinprodukte nach der Verordnung (EU) 2017/745 gelten: nein, da die vertikale bzw. sektorale Regelung für Medizinprodukte vorrangig zur Anwendung kommt. Falls keine Medizinprodukte, dann gilt der CRA.

 # Wie unterscheiden wir Produkte und Dienstleistungen? DL sind ja auch eigentlich Produkte.

In Art. 3 Z. 1 der VO wird der Begriff „Produkt" definiert als *„Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in den Verkehr gebracht werden."*

Dienstleistungen sind somit ausdrücklich nicht von der VO umfasst.

 # Als großes Industrie-Unternehmen stehen wir nun vor dem Problem, dass Zulieferfirmen ab 2027 bestimmte Teile nicht mehr verkaufen werden, da diese nicht CRA-konform sind. Bei langen Produktentwicklungszyklen von über 3 Jahren können wir nun die Produktion nicht einfach umstellen. Wie steht der Regulator beim CRA zu langen und komplexen Lieferketten?

Daher gibt es den relativ langen Zeitraum zwischen Inkrafttreten und voller Geltung der VO von knapp über drei Jahren. Grundsätzlich gilt für Bestand bzw. Produkte, die vor der vollen Geltung auf den Markt gebracht werden auch nach 2027 keine Pflicht zur Compliance, solange nicht danach wesentliche Änderungen am Produkt vorgenommen werden, die eine Neubewertung notwendig machen. Dasselbe gilt auch für Ersatzteile für Bestandsprodukte. Es wird notwendig sein, Lieferanten proaktiv auf das Thema anzusprechen, vertragliche Vereinbarungen zu treffen oder Alternativen zu suchen. Dass dies ein komplexes und zum Teil problematisches Thema werden kann, ist uns bewusst.

 # Ist Security by Design nicht noch wichtiger/schwerer als Schwachstellenmanagement?

Das ist wohl Geschmacksache und natürlich auch von den Erfahrungen im Team abhängig.

Wir haben uns bei der Top-3-Liste für das Schwachstellenmanagement entschieden, weil hier mehr langfristige Aufgaben auf den Hersteller warten.

 # Wie sehr werden wir uns künftig auf VEX (im Kontext von SBOM) verlassen können, um irrelevante Schwachstellen in 3rd-Party-Dependencies effizient wegfiltern zu können?

Effizienter wird es sicher werden, dank neuer Metriken wie EPSS (Exploit Prediction Scoring System) und KEV (Known Exploitable Vulnerabilities).

Vollständig automatisiert wird dies aber nie funktionieren können. Man muss hier ausreichende Ressourcen und kompetentes Personal haben.

 # Wenn ich als User kritischer Infrastruktur schon potenziell CRA-relevantes im Einsatz habe (also Bestand): muss ich selbst darauf evaluieren oder der Lieferant mich darauf hinweisen?

Eine aktive Hinweispflicht für CRA-Relevanz von Bestandsprodukten sehen wir derzeit nicht. Aus unserer Sicht muss ein Hersteller die Informationen nach Anhang II der VO zur Verfügung stellen. Nach Art. 8 Abs 2 lit. a der VO können per delegiertem Rechtsakt weitere Produkte, bei denen eine kritische Abhängigkeit von Einrichtungen nach der RL 2022/2555 (NIS2) besteht, zu „kritischen" Produkten nach CRA erklären. Das würde die Transparenz entsprechend erhöhen. Der CRA betrifft zwar die Hersteller bzw. Händler/Inverkehrbringer und nicht die Nutzer:innen; Bestand (Produkte, die vor der vollen Geltung der VO auf den Markt kommen) ist jedoch von der Geltung der VO ausgenommen, solange nach 2027 nicht wesentliche Änderungen am Produkt vorgenommen werden. Im Kontext kann es daher als Nutzer:in/Einrichtung der kritischen Infrastruktur sinnvoll sein, Lieferanten proaktiv auf das Thema anzusprechen.

 # Wie sinnvoll sehen Sie COBIT für SW-Entwicklungsprozessen im Vergleich zu OWASP SAMM?

Wir arbeiten am liebsten mit OWASP SAMM, weil es frei verfügbar, erfahrungsgemäß leicht zu lernen und allgemein anerkannt ist.

Essenziell ist, einen strukturiert aufgesetzten SDLC zu haben und zu pflegen, egal nach welchem Modell. Wenn COBIT schon erfolgreich im Einsatz ist, spricht nichts dagegen dabei zu bleiben.

 # Fallen Apps unter den CRA, wenn diese grundsätzlich kostenlos angeboten werden, aber im Kontext eines kommerziellen Angebots verwendet?

Ja.

Vgl. Erw.Gr. 15: *„Diese Verordnung gilt für Wirtschaftsakteure nur in Bezug auf Produkte mit digitalen Elementen, die auf dem Markt bereitgestellt werden, d. h., die im Rahmen einer Geschäftstätigkeit zum Vertrieb oder zur Verwendung auf dem Unionsmarkt geliefert werden. Eine Lieferung im Zusammenhang mit einer Geschäftstätigkeit ist möglicherweise nicht nur dadurch gekennzeichnet, dass für ein Produkt mit digitalen Elementen ein Preis verlangt wird, sondern auch dadurch, dass für technische Unterstützungsleistungen ein Entgelt verlangt wird, das nicht nur der Deckung der tatsächlichen Kosten dient, dass eine Gewinnerzielungsabsicht besteht, beispielsweise durch Bereitstellung einer Softwareplattform, über die der Hersteller andere Dienste gewinnorientiert anbietet, […]“.*