ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Der EU Cyber Resilience Act: Ein Überblick aus rechtlicher Sicht

Steven Arzt
Leonie Fischer
Michael Kreutzer
Kirstin Scheel
Markus Schneider
Linda Schreiber
Annika Selzer

Version 1.0
März 2024

Der EU Cyber Resilience Act: Ein Überblick aus rechtlicher Sicht

Impressum

Kontakt

Nationales Forschungszentrum für
angewandte Cybersicherheit ATHENE
c/o Fraunhofer-Institut für
Sichere Informationstechnologie SIT
Rheinstraße 75
64295 Darmstadt

Autoren

Steven Arzt,
Leonie Fischer,
Michael Kreutzer,
Kirstin Scheel,
Markus Schneider,
Linda Schreiber,
Annika Selzer

Förderhinweis

Dieser Beitrag wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) und des Hessischen Ministeriums für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.

Des Weiteren wurde die Erstellung unterstützt durch das BMBF-Projekt StartupSecure und von der Förderung des European Digital Innovation Hub EDITH vom European Commission's Digital Europe Programme.

Hinweise zur Haftung

Die in diesem Beitrag enthaltenen Informationen sind sorgfältig erstellt worden, können eine Rechtsberatung jedoch nicht ersetzen. Eine Haftung oder Garantie dafür, dass die Informationen die Vorgaben der aktuellen Rechtslage erfüllen, wird daher nicht übernommen.

Gleiches gilt für die Brauchbarkeit, Vollständigkeit oder Fehlerfreiheit, sodass jede Haftung für Schäden ausgeschlossen wird, die aus der Benutzung dieser Arbeitsergebnisse/Informationen entstehen können. Diese Haftungsbeschränkung gilt nicht in Fällen von Vorsatz.

Lesehinweise

Grundsätzlich bezieht sich dieses Whitepaper auf den Stand der CRA-Entwurfsversion vom 12.03.2024.[1] Es liegt jedoch noch keine final verabschiedete Version des Verordnungstextes vor.

Beim CRA wird es sich um eine EU-*Verordnung* handeln. Neben Verordnungen gibt es Richtlinien als weitere Form von Rechtsakten in der EU-Gesetzgebung. Richtlinien müssen von den Mitgliedstaaten jeweils in eigenes nationales Recht umgesetzt werden, dagegen gelten Verordnungen direkt und unmittelbar in allen Mitgliedstaaten. Dies bedeutet, dass der CRA-Verordnungstext mit seinen Verpflichtungen **direkt bindend** für betroffene Akteure ist. Beim CRA handelt es sich um einen „Text von Bedeutung für den EWR", dies bedeutet, dass die Bestimmungen des CRA sowohl für die EU-Mitgliedsstaaten als auch zusätzlich für die Staaten des Europäischen Wirtschaftsraums (EWR) Island, Liechtenstein und Norwegen relevant sein werden. Zur besseren Lesbarkeit wird in diesem Whitepaper nur von der EU gesprochen.

Der CRA gliedert sich in den eigentlichen Verordnungstext und die sog. Erwägungsgründe (Erwgr.). Der Verordnungstext besteht aus Artikeln, die die verbindlichen, unmittelbar anzuwendenden Vorschriften enthalten, die von den Betroffenen befolgt bzw. wahrgenommen werden müssen. Dagegen dienen die Erwägungsgründe dazu, den Kontext, die Ziele und Überlegungen hinter den einzelnen Regelungen des CRA zu verdeutlichen. Die Erwägungsgründe bieten eine Orientierungshilfe für die Auslegung und Anwendung des CRA, haben aber keine direkte rechtliche Wirkung.

Im Whitepaper sind direkte Bezugnahmen auf den Wortlaut des CRA im Text durch Referenz auf die genaue Fundstelle in der CRA-Entwurfsversion kenntlich gemacht. Dies bedeutet, dass im Satz selbst ein expliziter Verweis auf den spezifischen Artikel, Absatz oder Erwägungsgrund der Verordnung erfolgt. Dies ermöglicht es, den genauen Kontext und die genaue Formulierung der Regelung nachzuvollziehen und sie bei Bedarf direkt im Verordnungstext nachzuschlagen.

Unter https://www.athene-center.de/cra werden ggf. aktualisierte Fassungen des Whitepapers zur Verfügung gestellt.

Aus Gründen der besseren Lesbarkeit wird im vorliegenden Dokument auf die Verwendung männlicher und weiblicher Sprachformen verzichtet. Es wird das generische Maskulinum verwendet, wobei alle Geschlechter gleichermaßen gemeint sind.

[1] abrufbar unter: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_DE.pdf

Inhalt

Vorwort

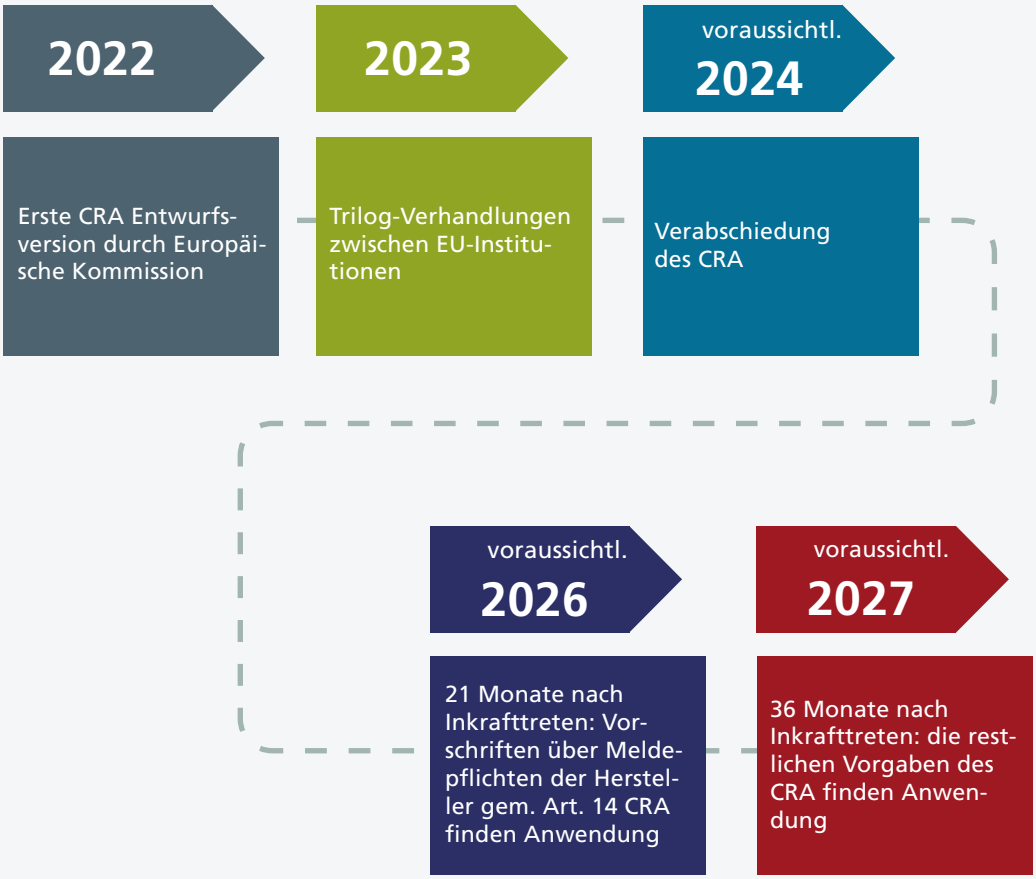

Abbildung 1: Timeline CRA

Die Europäische Kommission hat am 15.09.2022 einen ersten Vorschlag für die *Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen*, den sog. **Cyber Resilience Act** (im Folgenden CRA) vorgelegt (zur Timeline siehe *Abbildung 1*). Im Rahmen der folgenden Trilog-Verhandlungen zwischen den EU-Institutionen wurden der Vorschlag sowie verschiedene Änderungsentwürfe umfassend diskutiert, bis Ende 2023 eine **vorläufige Einigung** auf politischer Ebene erzielt wurde.[2] Am 12.03.2024 wurde der CRA durch das Europäische Parlament verabschiedet. Es wird erwartet, dass der CRA im Laufe des Jahres 2024 in Kraft tritt, vorher muss er vom Rat der EU offiziell angenommen werden.[3] Sobald der CRA in Kraft tritt, gilt er mit entsprechenden Umsetzungsfristen in

[2] Europäischer Rat, https://www.consilium.europa.eu/de/press/press-releases/2023/11/30/cyber-resilience-act-council-and-parliament-strike-a-deal-on-security-requirements-for-digital-products/

[3] Europäisches Parlament, https://www.europarl.europa.eu/news/de/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products

allen EU-Mitgliedsstaaten und wird sich insbesondere auf Hersteller von einschlägigen Produkten sowie andere Wirtschaftsakteure auswirken, die diese Produkte in der EU absetzen möchten.

Dieses Whitepaper richtet sich an alle, die sich einen ersten **Überblick über die Regelungen des CRA** verschaffen wollen und insbesondere an Personen, die in ihren Organisationen für die Entwicklung, Herstellung oder den Vertrieb von Produkten mit digitalen Elementen verantwortlich sind. Für Organisationen ist es ratsam, sich frühzeitig mit den Regelungen des CRA vertraut zu machen. Im ersten Schritt ist zu klären, inwiefern der CRA auf eine Organisation und die von ihr hergestellten oder vertriebenen Produkte Anwendung findet. Vor diesem Hintergrund liegt der Schwerpunkt dieses Whitepapers auf der Frage **„Für wen, was und wo gilt der CRA?“** (siehe Abschnitt A dieses Dokuments). Zudem erfolgt ein **Überblick zu den Aufgaben und Pflichten** der verschiedenen unter dem CRA verpflichteten Akteure (siehe B.), den verschiedenen **Sicherheitsstufen** bei Produkten mit digitalen Elementen, die unter dem CRA unterschieden werden (siehe C.), und den möglichen **Sanktionen** bei einem Verstoß gegen den CRA (siehe D.).

Ein weiteres Whitepaper von ATHENE zu ausgewählten technischen Anforderungen des CRA und mit Umsetzungsempfehlungen und Erläuterungen ist in Vorbereitung. Dieses richtet sich insbesondere an Herstellerorganisationen.

Management Summary

Der EU Cyber Resilience Act (CRA) wird voraussichtlich im Laufe des Jahres 2024 verabschiedet werden. Nach einer Umsetzungsfrist von 21 bzw. 36 Monaten gelten dann **europaweit einheitliche, branchen- und bereichsübergreifende Anforderungen für die Cybersicherheit von vernetzten Hard- und Softwareprodukten**. Dieser umfassende Regulierungsansatz des CRA wird viele Unternehmen erstmalig mit Vorschriften zur Cybersicherheit betreffen, die durch bisherige produkt-, verbraucher- oder sektorspezifische Regelungen nicht erfasst sind.

Damit ihre Produkte weiterhin erfolgreich am Markt bestehen können und zukunftsfähig bleiben, sollten sich **Hersteller von Produkten mit digitalen Elementen** frühzeitig mit den Anforderungen des CRA befassen. Auch wenn die finale Version des CRA noch nicht vorliegt, gibt es verschiedene Anforderungen, mit denen sich Unternehmen bereits jetzt auseinandersetzen können. Durch die künftigen gesetzlichen Anforderungen müssen sie ggf. ihre Sicherheitsstandards erhöhen und ihre Produkte widerstandsfähiger gegenüber Cyberangriffen machen. Dies stärkt nicht nur das Vertrauen von Kunden, sondern verbessert auch die Produktqualität sowie die internationale Wettbewerbsfähigkeit. Der CRA wird voraussichtlich auch dazu führen, dass die Nachfrage nach Produkten mit transparenten Cybersicherheitseigenschaften verstärkt wird.

Die Vorschriften des CRA betreffen **Produkte, die im EU-Markt angeboten und vertrieben werden**, und richten sich in erster Linie an die Hersteller dieser Produkte – unabhängig davon, ob diese selbst in der EU niedergelassen sind oder nicht. Um eine lückenlose Durchsetzung der CRA-Anforderungen sicherzustellen, werden neben Herstellern auch weitere Akteure (sog. **Einführer** und **Händler**) entlang der Lieferkette betroffener Produkte verpflichtet.

Die Anforderungen des CRA gelten für den **gesamten Lebenszyklus eines betroffenen Produktes**: Die Cybersicherheitsauflagen des CRA müssen ab der Konzeptionsphase und über einen Support-Zeitraum von regelmäßig mindestens fünf Jahren erfüllt werden. Darüber hinaus verpflichtet der CRA die Hersteller dazu, die Transparenz von Cybersicherheitseigenschaften zu verbessern, um Nutzer zur sicheren Verwendung entsprechender Produkte zu befähigen. Der CRA schreibt zudem Prozesse für eingehende Schwachstellenmeldungen und Sicherheitsvorfälle vor. Verstöße gegen den CRA können vergleichbar mit den DSGVO-Bußgeldregeln mit bis zu 2,5% des gesamten weltweiten Jahresumsatzes sanktioniert werden.

Dieses Whitepaper bietet eine kompakte Zusammenfassung von zentralen Bestimmungen des CRA, die es ermöglichen soll, die wesentlichen Inhalte des CRA zu verstehen, ohne dafür in die detaillierten Einzelheiten der Verordnung einsteigen zu müssen. Es ist zu beachten, dass sich die Informationen in diesem Whitepaper auf eine Version des Verordnungstextes beziehen, die noch nicht final verabschiedet wurde (Stand 12.03.2024).

Unter https://www.athene-center.de/cra findet man aktuelle Hinweise zu Veranstaltungen, Ansprechpartnern und weitere Informationen zum CRA sowie ggf. eine aktualisierte Version dieses Dokuments.

A. Für wen, was und wo gilt der CRA?

Der CRA soll branchenübergreifend einheitliche, horizontale Regelungen schaffen. Diese gelten für **Produkte mit digitalen Elementen, die im B2B- und B2C-Bereich** eingesetzt werden. Hiervon umfasst sind sowohl Software als auch Hardware und vernetzte, physische Produkte, die Datenverbindungen mit einem Gerät oder Netz aufbauen können, sowie Komponenten hiervon, die getrennt in den Verkehr gebracht werden. Dies betrifft Produkte mit digitalen Elementen, die **innerhalb der EU bereitgestellt** werden und kann damit auch Hersteller betreffen, die selbst keinen Sitz in der EU haben. Der CRA verpflichtet **Hersteller sowie weitere Akteure entlang der Lieferkette (sog. Einführer und Händler, siehe A. 2)** von Produkten mit digitalen Elementen zur Einhaltung von Cybersicherheitsanforderungen.

Im folgenden Kapitel werden diese Begrifflichkeiten und Voraussetzungen für die Anwendbarkeit des CRA im Detail betrachtet.

1. Welche Produkte werden vom CRA reguliert?

1.1 Produkte mit digitalen Elementen – was fällt darunter?

Der CRA findet Anwendung auf sowohl materielle als auch immaterielle Produkte mit digitalen Elementen, deren bestimmungsgemäße oder vorhersehbare Verwendung eine direkte oder indirekte logische oder physische **Datenverbindung** mit einem Gerät oder Netz einschließt (Art. 2 Abs. 1 CRA). Gemäß Art. 3 Nr. 1 CRA handelt es sich bei einem Produkt mit digitalen Elementen **sowohl um Software als auch um Hardware und die dazugehörigen „Datenfernverarbeitungslösungen, einschließlich Soft- oder Hardwarekomponenten, die getrennt in den Verkehr gebracht werden“** (zum Begriff der Datenfernverarbeitungslösungen, siehe 1.4). Der Anwendungsbereich des CRA erfasst somit Soft- und Hardware als Formen oder Bestandteile von elektronischen Informationssystemen, die digitale Daten verarbeiten, speichern oder übertragen können (Art. 3 Nr. 4, 5 und 7 CRA).[4,5]

Mit welcher Art von Netz bzw. System ein Produkt gemeinhin verbunden wird, wird im CRA nicht weiter spezifiziert. Auch wenn das Produkt normalerweise nur in abgetrennten (“air-gapped”) Netzen ohne Verbindung zum Internet betrieben

[4] *Rockstroh*: EU-Cybersicherheitsrecht für Produkte, in: DuD 2023, S.333; *Wiebe; Daelen*: Der Cyber Resilience Act aus produktsicherheitsrechtlicher Perspektive, in: EuZW 2023, 257, 258.

[5] Der Begriff „Produkt mit digitalen Elementen“ ist ein eigenständiger Begriff des CRA und nicht zu verwechseln mit ähnlichen Begriffen aus anderen Gesetzgebungen, wie bspw. den „Waren mit digitalen Elementen“ aus der Warenkauf-Richtlinie (EU) 2019/771.

wird, wie es z.B. in manchen industriellen Steuersystemen oder in Kraftwerken der Fall ist, ist davon auszugehen, dass es sich um eine Datenverbindung handelt und entsprechende Produkte in den Anwendungsbereich fallen.

1.2 Welche Produktkategorien fallen unter den CRA?

Die Definition von Produkten mit digitalen Elementen und der Anwendungsbereich des CRA sind damit sehr umfassend. Nicht abschließende Produktkategorien, die dazugehören, sind:

- mobile Geräte, z.B. Laptops, Smartwatches, vernetzte Spielzeuge
- IoT-Geräte, z.B. intelligente Stromzähler, Thermostate, Steuerungen für Jalousien
- Netzwerkinfrastrukturgeräte, z.B. Router, Switches, Gateways
- Vernetzte industrielle Steueranlagen (Industrie 4.0), z.B. fernsteuerbare bzw. fernwartbare Maschinen, (teil-)autonome Roboter, steuerbare Förderanlagen
- Software, die lokal auf elektronischen Geräten installiert wird, z.B. Treiber, Apps, Office-Programme

1.3 Welche Produkte sind vom Anwendungsbereich des CRA ausgenommen?

Vom Anwendungsbereich des CRA **ausgenommen** (Art. 2 Abs. 2 bis 4, 7 CRA) sind Produkte mit digitalen Elementen:

- die unter die Verordnung für **Medizinprodukte** (Verordnung (EU) 2017/745),
- die Verordnung über **In-vitro-Diagnostika** (Verordnung (EU) 2017/746),
- die Verordnung über die **Typengenehmigung von Kraftfahrzeugen** (Verordnung (EU) 2019/2144) fallen,
- die nach der Verordnung über gemeinsame Vorschriften zur **Zivilluftfahrt** (Verordnung (EU) 2018/1139) zertifiziert wurden,
- die in den Anwendungsbereich der Richtlinie über **Schiffsausrüstung** (Richtlinie 2014/90/EU) fallen,
- die ausschließlich für Zwecke der **nationalen Sicherheit oder Verteidigung** entwickelt oder angepasst wurden.

Gemäß Art. 2 Abs. 5 CRA kann die Anwendung des CRA weiterhin ausgeschlossen bzw. eingeschränkt werden, wenn ein Produkt mit digitalen Elementen bereits sektorspezifischen Vorschriften unterfällt und diese mindestens dasselbe Schutzniveau aufweisen wie der CRA. Der Europäischen Kommission wird die Befugnis übertragen, diese Entscheidungen zur Einschränkung der Anwendbarkeit mittels delegierten Rechtsakten zu treffen. Dabei ist zu beachten, dass nur spezifische Arten von Produkten ausgenommen werden können, nicht aber ganze Sektoren.

Darüber hinaus soll der CRA nach Art. 2 Abs. 6 CRA keine Anwendung auf Komponenten finden, die ausschließlich zu dem Zweck hergestellt werden, als **Ersatzteile** identische Komponenten zu ersetzen und die vom Hersteller des Originalproduktes im Rahmen derselben Entwicklungs- und Produktionsprozesse wie das Originalprodukt hergestellt wurden. Somit können alte Produkte weiterhin in Betrieb gehalten werden, auch wenn diese Produkte nach Inkrafttreten des CRA so nicht mehr neu an den Markt gebracht werden dürften. Dies dürfte insbesondere für Produkte mit langer Lebens-/Nutzungsdauer wie bspw. industrielle Fertigungsmaschinen relevant sein.

1.4 Fällt Software as a Service (SaaS) in den Anwendungsbereich des CRA?

Der CRA bezieht sich auf Produkte mit digitalen Elementen, nicht aber auf Dienstleistungen. Zur Unterscheidung im Kontext von SaaS-Anwendungen ist ein Blick auf die entsprechenden CRA-Definitionen zu werfen: Der **CRA bezieht sich auf Soft- und Hardwareprodukte und deren (dazugehörige) *Datenfernverarbeitungslösungen*** (Art. 3 Nr. 1 CRA). Der Begriff Datenfernverarbeitungslösung meint im CRA „jede entfernt stattfindende Datenverarbeitung, für die eine Software vom Hersteller selbst oder unter dessen Verantwortung konzipiert und entwickelt wurde und ohne die das Produkt **eine seiner Funktionen nicht erfüllen könnte**“ (Art. 3 Nr. 2 CRA). Hintergrund dieser Regelung ist, dass Produkte mit digitalen Elementen in ihrer Gesamtheit durch den Hersteller gesichert werden. Hierfür ist es unerheblich, ob eine Software lokal auf dem Gerät des Nutzers oder aus der Ferne durch den Hersteller ausgeführt wird (Erwgr. 11 CRA).

Cloud-Lösungen fallen also nur dann in den Anwendungsbereich des CRA, wenn sie diese Definition von Datenfernverarbeitungslösungen erfüllen (Erwgr. 12 CRA). Dies ist beispielsweise bei vielen Lösungen im Smart-Home-Bereich der Fall: Bei einem smarten Kühlschrank müssen die CRA-Pflichten für das Gerät selbst (Hard- und Software) sowie für jede Datenfernverarbeitung, die zusätzliche Funktionalitäten cloud-basiert ermöglicht (bspw. Rezeptvorschläge auf Basis des Inhalts des Kühlschranks), erfüllt werden.

Im Einzelfall kann die **Abgrenzung zwischen Dienstleistung und Produkt mit digitalen Elementen bei Clouddiensten und SaaS-Lösungen** komplex sein und eine individuelle Bewertung erfordern.

1.5 Wann wird Open-Source-Software (OSS) vom CRA erfasst?

Der CRA betrifft Produkte mit digitalen Elementen, die auf dem EU-Markt bereitgestellt werden. Unter Bereitstellung versteht man jede entgeltliche oder unentgeltliche Abgabe eines Produktes zum Vertrieb oder zur Verwendung **im Rahmen einer Geschäftstätigkeit** (Art. 3 Nr. 22 CRA).

Die Regulierung von Open Source ist einer der Bereiche des CRA, über die am heftigsten diskutiert wurde. In der aktuellen Entwurfsversion wird die Kernfrage der Geschäftstätigkeit in Zusammenhang mit Open Source (s.u.) im Interessensausgleich adressiert. Die nachfolgenden Ausführungen sollten dementsprechend

wahrscheinlich auch nach Verabschiedung des CRA gelten.

Über die vergangenen drei Jahrzehnte hinweg ist die Bedeutung von Open Source für kommerzielle Unternehmen enorm gestiegen. Beispiele hierfür:

- In vielen kommerziellen Produkten werden Open-Source-Komponenten eingesetzt. Hierzu zählen z.B. Logging-Frameworks oder Bibliotheken zum Einlesen von Dateiformaten.
- Unternehmen beteiligen sich an der Open-Source-Entwicklung, z.B. um Industriestandards gemeinsam mit Partnern nur einmal für alle zu implementieren und so den Entwicklungsaufwand für jeden einzelnen Partner zu senken, während gleichzeitig die Kompatibilität entlang der Zulieferkette sichergestellt wird.
- Gerade im Startup-Bereich sind Open-Source-Geschäftsmodelle zu finden, bei denen der Ertrag nicht klassisch über Softwarelizenzen erfolgt, sondern z.B. über Wartung und Schulung.
- Unternehmen vertreiben Hardware, z.B. einen Router oder ein Smart-TV-Gerät, während die darauf installierte Software komplett aus bestehender Open-Source-Softwarezusammengesetzt ist und nicht von einem Unternehmen entwickelt wurde.

Bei allen o.g. Beispielen stellt sich die Frage, wann von einer Geschäftstätigkeit auszugehen ist und das Produkt somit unter den CRA fällt. Geschäftstätigkeit meint grundsätzlich eine Bereitstellung im unternehmensbezogenen Kontext und schließt verschiedene Ausgestaltungen kommerzieller Aktivität ein, wobei die Software nicht unmittelbar die Leistung sein muss, für die bezahlt wird (Erwgr. 15 CRA). Ob ein Produkt mit digitalen Elementen im Rahmen einer Geschäftstätigkeit bereitgestellt wurde und damit der CRA Anwendung findet, ist im Einzelfall unter Berücksichtigung verschiedener Faktoren (Regelmäßigkeit der Bereitstellung, Eigenschaften des Produktes, Absichten der Akteure etc.) zu prüfen.[6] Ebenso ist zu klären, welche Pflichten sich beim Einsatz von OSS für Hersteller ergeben.

1.5.1 Inwiefern werden Open-Source-Komponenten vom CRA erfasst?

Wird eine Open-Source-Komponente (z.B. log4j) im Produkt eines Herstellers **eingesetzt**, muss das Gesamtprodukt einschließlich der OSS-Komponente die Mindestsicherheitsanforderungen des CRA erfüllen und der Hersteller ist für das Gesamtprodukt einschließlich dieser Komponenten verantwortlich (Art. 13 Abs. 1 und 5 CRA). Der CRA sieht die Möglichkeit vor, solche Komponenten zentralisiert zu bewerten. Dieses Thema wird in diesem Dokument später im Kontext der sogenannten *Verwalter quelloffener Software* (engl. Open-Source-Stewards) behandelt.

[6] Europäischen Kommission, Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 („EU Blue Guide"), S. 19.

Software kann **Bestandteil eines Geräts** sein, welches verkauft wird. Angenommen ein Unternehmen entwickelt eine Open-Source-Firmware für DSL-Router, die jeder kostenlos herunterladen und auf beliebigen Routern installieren kann. Gleichzeitig verkauft das Unternehmen aber auch Router mit vorinstallierter Firmware. In diesem Fall wäre davon auszugehen, dass der Verkauf der Router, die ohne die Firmware unbrauchbar wären, eine Geschäftstätigkeit ist, womit auch die Firmware dem CRA unterliegen würde.

1.5.2 Inwiefern werden Open-Source-Geschäftsmodelle vom CRA erfasst?

Open-Source-Software kann im Rahmen einer **kommerziellen Aktivität** gegen Geld lizenziert werden. Viele weit verbreitete Open-Source-Lizenzen treffen keine Aussage über den Preis. Sie garantieren dem Nutzer lediglich bestimmte Freiheiten wie z.B. den Zugang zum Quellcode und die Möglichkeit, Änderungen vorzunehmen und diese mit anderen zu teilen. Wird die Software kostenpflichtig angeboten oder ist sie nur im Rahmen eines kostenpflichtigen Wartungsvertrags erhältlich (dies wäre bspw. bei RedHat Enterprise Linux anzunehmen), handelt es sich um eine Bereitstellung im Rahmen einer Geschäftstätigkeit (Erwgr. 15 CRA). Somit treffen den Hersteller dieselben Verpflichtungen aus dem CRA wie bei einem Produkt, das nicht unter einer Open-Source-Lizenz steht. Ebenso verhält es sich mit sogenannten **"Dual License"-Modellen**, bei denen z.B. Privatnutzern eine kostenlose Open-Source-Lizenz und Unternehmenskunden eine kostenpflichtige Lizenz angeboten wird (dies wiederum wäre bspw. bei MySQL anzunehmen).

Im Zusammenhang mit Open-Source-Software ist die Annahme von **Spenden ohne Gewinnerzielungsabsicht zur Deckung der tatsächlichen Kosten** für die Gestaltung, Entwicklung und Bereitstellung des Open-Source-Produktes, nicht als Geschäftstätigkeit zu sehen (Erwgr. 15 CRA). Dies ist grundsätzlich auch der Fall, wenn die finanzielle Unterstützung von gewinnorientierten Unternehmen stammt. Nutzt ein Smart-TV-Hersteller bspw. Linux in seinem Gerät und unterstützt deswegen die Linux Foundation personell und/oder finanziell zum Ausbau der Linux-Multimedia-Funktionalität, führt dies offenbar nicht automatisch zur Annahme einer Geschäftstätigkeit und damit Anwendbarkeit des CRA für Linux.

Eine **Software selbst kann kostenlos** angeboten werden mit dem Ziel, beispielsweise kostenpflichtige Schulungen, Wartungsverträge oder Installationsdienste zu der Software anzubieten oder ein **Ökosystem bzw. eine Plattform** zu schaffen, an dem der Hersteller anderweitig verdient (Erwgr. 15). Obwohl der Kunde prinzipiell die kostenlose Software nutzen und keine weiteren Dienste in Anspruch nehmen kann, beruht die wirtschaftliche Tätigkeit des Herstellers letztlich indirekt auf der Software, die ihm überhaupt erst ermöglicht, diese Einnahmen im „Sekundärgeschäft" zu erzielen. In diesem Fall fällt das an sich kostenlose Produkt dennoch unter den CRA.

Auch **werbefinanzierte Modelle** können durch die **indirekte kommerzielle Nutzung** dem CRA unterfallen, bspw. wenn eine Handy-App kostenlos angeboten wird, jedoch Werbung anzeigt. Werden als Voraussetzung für die Nutzung von Open-Source-Software personenbezogene Daten verarbeitet, zu anderen Zwecken als ausschließlich der Verbesserung der Sicherheit, Kompatibilität oder Interoperabilität der Software, spricht dies ebenso für eine Bereitstellung im Rahmen

einer Geschäftstätigkeit und damit die Anwendbarkeit des CRA (Erwgr. 15 CRA).

Diese Fokussierung auf die **Gewinnerzielungsabsicht** schafft gleichzeitig die Unterscheidung zwischen Unternehmen mit Open-Source-Geschäftsmodell und reinen nicht-kommerziellen Open-Source-Projekten (siehe hierzu vertiefend Info: Exkurs Open-Source-Projekt).

Um die Besonderheiten von Open-Source-Entwicklung und-Einsatz interessensgerecht zu berücksichtigen, wurde in der aktuellen Entwurfsversion des CRA die Rolle der „Verwalter quelloffener Software" (siehe B.2.) vorgeschlagen. Diese Rolle sieht spezielle und vereinfachte Regelungen für Organisationen vor, die Open-Source-Software Projekte betreuen.

Info: Exkurs Open-Source-Projekte

Die Bereitstellung auf dem Markt im Rahmen einer Geschäftstätigkeit setzt im Kontext des CRA voraus, dass der Hersteller direkt eine kommerzielle Aktivität bzw. Absicht verfolgt, die Software zu monetarisieren, was über die reine gemeinnützige, allenfalls die eigenen Kosten deckende Bereitstellung der Software hinausgeht (Erwgr. 15 CRA).

Viele Open-Source-Projekte sind nicht mit einer Gewinnerzielungsabsicht verbunden. Die Kerngruppe, welche diese Software betreut, agiert gemeinnützig und stellt die Open-Source-Software kostenfrei inklusive des Quellcodes für die Allgemeinheit zur Verfügung und erlaubt die Nutzung, Veränderung und Weiterverbreitung ("Free and Open-Source-Software – FOSS"). Diese FOSS-Modelle definieren sich unter dem CRA dadurch, dass etwaige Einnahmen, wie Spenden, wieder den gemeinnützigen Zielen, also der Weiterentwicklung des Open-Source-Projektes, zufließen (Art. 3 Nr. 48 CRA). Stellt die Organisationsform eines Open-Source-Projekts diese Bedingungen (FOSS, Mittelrückfluss zur gemeinnützigen Tätigkeit) sicher, handelt sie nicht im Rahmen einer Geschäftstätigkeit, womit solche Software regelmäßig nicht dem CRA unterliegt (Erwgr. 18 CRA).

In der Praxis werden Open-Source-Komponenten im Kern von gemeinnützigen Initiativen getragen, erhalten jedoch signifikante Beiträge von gewinnorientierten Marktakteuren. So beteiligen sich Unternehmen wie z.B. RedHat oder Canonical massiv an der Weiterentwicklung des Linux-Kernels und vieler Open-Source-Anwendungen im Linux-Umfeld. Dies geschieht durch die Bereitstellung von Personal, durch Spenden oder durch den Betrieb von Servern z.B. für sogenannte Download-Mirrors. Offenbar agieren diese gewinnorientieren Marktakteure damit aus kommerziellen Beweggründen, weil die Open-Source-Komponenten anschließend als Bausteine in den kommerziellen Produkten dieser Unternehmen zum Einsatz kommen. Insofern ist hier davon auszugehen, dass die Produkte von RedHat und Canonical vom CRA erfasst werden.

Diese spätere Verwertung ändert jedoch nichts daran, dass das Open-Source-Projekt im Kern gemeinnützig ist und bleibt. Im CRA wird hierfür die Trennung von Entwicklung und Verwertung hervorgehoben: Die Ergebnisse des Open-Source-Projekts stehen der Allgemeinheit kostenfrei (FOSS) zur Verfügung, auch wenn einzelne Beitragende darauf aufbauend kommerzielle Aktivitäten durchführen (Erwgr. 18). Auch wenn RedHat-Linux kommerziell ist und RedHat-Entwickler am Linux-Kernel mitarbeiten, führt dies voraussichtlich nicht zu einer Anwendbarkeit des CRA für den Linux-Kernel selbst. Der Linux-Kernel wird aktuell nicht mit dem Ziel weiterentwickelt, direkt oder indirekt Einnahmen zu erzielen. Die hierfür maßgebliche Organisation, die Linux Foundation, ist ein gemeinnütziger

Verein und besteht unabhängig von den wirtschaftlichen Aktivitäten ihrer gewinnorientierten Unternehmenspartner. Dies soll als Beispiel veranschaulichen, dass mit dem CRA nicht beabsichtigt wird, solche Initiativen zu regulieren, damit es keine Hürden für die Weiterentwicklung gibt.

Es handelt sich hierbei um ein Spannungsfeld, über das vermutlich erst nach dem Geltungsbeginn des CRA Klarheit geschaffen werden wird. Viele Open-Source-Projekte werden federführend von gewinnorientierten Akteuren getragen, z.B. wenn diese den Großteil der Entwickler beisteuern. Selbst wenn ein Open-Source-Projekt ohne die Beiträge der gewinnorientierten Unternehmen nicht überlebensfähig wäre, bedingt dies nicht notwendigerweise eine Geschäftstätigkeit des Open-Source-Projektes.

1.6 Inwiefern fallen Legacy-Produkte unter den CRA?

Nach dem Inkrafttreten des CRA gilt eine **Umsetzungsfrist von 36 Monaten bzw. 21 Monaten** für die Meldepflichten der Hersteller nach Art. 14 CRA (Art. 71 Abs. 2 CRA). Für den Übergang wird in Art. 69 Abs. 2 CRA geregelt, dass Produkte, die vor Ablauf der Umsetzungsfrist in den Verkehr gebracht werden, nur den Anforderungen des CRA unterliegen, wenn nach Ablauf der Umsetzungsfrist wesentliche Änderungen (siehe A.2.1) am Produkt durchgeführt werden.

Dies bedeutet, dass Produkte, die bereits jetzt und vor Ablauf der Frist in den Verkehr gebracht wurden oder werden und bei denen nach Ablauf der Umsetzungsfrist keine nachträglichen wesentlichen Änderungen erfolgen, nicht den Anforderungen des CRA unterliegen.

Um die Lebensdauer von Produkten zu verlängern, sieht Art. 2 Abs. 6 CRA vor, dass für **Ersatzteile**, die etwa der Reparatur von sogenannten Legacy-Produkten dienen, eine Ausnahme vom Anwendungsbereich des CRA gewährt werden soll.

2. Welche Akteure werden unter dem CRA verpflichtet?

Der CRA stellt einen umfassenden Pflichtenkatalog für die betroffenen Wirtschaftsakteure auf. Gemäß Art. 3 Nr. 12 CRA sind diese **Wirtschaftsakteure** insbesondere **Hersteller, Bevollmächtigte, Einführer, Händler, Verwalter quelloffener Software** sowie jede andere natürliche oder juristische Person, die im Rahmen des CRA verpflichtet wird. Die Begriffsbestimmungen dieser verschiedenen Akteure entsprechen in ihrer Ausgestaltung den Definitionen anderer EU-Harmonisierungsrechtsvorschriften im Bereich Produktsicherheit.

Insbesondere bei betroffenen Produkten mit komplexen Vertriebswegen und Lieferketten sowie Berührungspunkten zu Drittstaaten außerhalb der EU ist es für die in Herstellung und Vertrieb involvierten Organisationen wichtig, sich früh mit den Definitionen dieser verschiedenen Rollen der Wirtschaftsakteure unter dem CRA auseinanderzusetzen. Die Aufgaben und Pflichten, die der CRA vorsieht,

hängen davon ab, welche der Rollen eine Organisation in Bezug auf ein Produkt einnimmt, Eine Organisation hat in Bezug auf ein Produkt mit digitalen Elementen regelmäßig nur jeweils eine der drei Rollen (Hersteller, Händler, Einführer) inne.

Verschiedene unternehmensstrategische Entscheidungen, wie die Vornahme von Änderungen an Produkten oder der Vertrieb unter dem Namen oder der Marke einer anderen als der Herstellerorganisation, können sich so unmittelbar auf die gesetzlichen Verpflichtungen an die jeweilige Organisation auswirken. Maßgeblich ist in diesem Zusammenhang häufig auch die Frage, welcher Akteur ein Produkt im Unionsmarkt *in den Verkehr gebracht* hat oder *bereitstellt*. Das Inverkehrbringen definiert sich als erstmaliges Bereitstellen eines Produktes im Unionsmarkt und kann folglich für jedes Produktexemplar nur einmal erfolgen. Zum Begriff der Bereitstellung im Unionsmarkt siehe folgenden Abschnitt „Wo findet der CRA räumlich Anwendung?“, siehe A.3.

Die konkreten Aufgaben und Pflichten der jeweiligen Akteure werden später in Kapitel B dargestellt, (siehe B.) sowie in einer Übersicht der aus dem CRA entstehenden Verpflichtungen für Hersteller, Bevollmächtigte, Einführer, Händler und Verwalter quelloffener Software im Anhang. Der folgende Abschnitt behandelt die Definition und Abgrenzung zwischen diesen Rollen.

2.1 Wer gilt unter dem CRA als Hersteller?

Als Akteure, die tatsächliche Entscheidungsgewalt bzw. Produktverantwortlichkeit übernehmen, stellen Hersteller den zentralen Adressaten der Verpflichtungen unter dem CRA dar. Gemäß Art. 3 Nr. 13 CRA ist ein Hersteller eine „natürliche oder juristische Person, die Produkte mit digitalen Elementen **entwickelt oder herstellt [bzw.] konzipieren, entwickeln oder herstellen lässt** und dieses Produkt unter dem **eigenen Namen oder eigener Marke vermarktet**, sei es entgeltlich oder unentgeltlich“. Ein Unternehmen gilt demnach auch als Hersteller, wenn die Entwicklungsarbeit nicht in-house, sondern durch einen externen Dienstleister oder Subunternehmer durchgeführt wird, wenn das Unternehmen das Produkt später unter eigenem Namen oder eigener Marke in den Verkehr bringt.

Zudem gelten Einführer und Händler dann als Hersteller und haben die entsprechenden Verpflichtungen als Hersteller zu erfüllen, wenn sie ein Produkt **unter ihrem Namen oder ihrer Marke in den Verkehr bringen** oder **wesentliche Änderungen** an einem bereits in Verkehr gebrachten Produkt vornehmen (Art. 21 CRA). Weiterhin gelten sonstige natürliche oder juristische Personen dann als Hersteller, wenn sie wesentliche Änderungen an einem Produkt mit digitalen Elementen vornehmen und das Produkt auf dem Markt bereitstellen (Art. 22 CRA). Solche wesentlichen Änderungen sind insbesondere dann gegeben, wenn sich dadurch der Verwendungszweck des Produktes ändert oder die Änderungen Auswirkungen auf die Erfüllung der Cybersicherheitsanforderungen nach Anhang I, Abschnitt 1 CRA durch das jeweilige Produkt hatten (Art. 3 Nr. 30 CRA).

Voraussetzung für die Eigenschaft als Hersteller ist demnach nicht, dass der Hersteller einen Sitz in der Union hat. Die Herstellerpflichten gelten daher **auch für Hersteller, die in einem Drittland außerhalb der EU** niedergelassen sind.[7]

Der Hersteller hat, unabhängig davon, ob dieser eine Niederlassung innerhalb der EU hat oder nicht, die Möglichkeit, schriftlich einen **Bevollmächtigten** i. S. v. Art. 3 Nr. 15 CRA zu benennen, der in der Union ansässig oder niedergelassen ist und im Namen des Herstellers bestimmte administrative Verpflichtungen erfüllt.[8] Nach Art. 18 Abs. 3 CRA soll es etwa Aufgabe des Bevollmächtigten sein, die Konformitätserklärung und die technische Dokumentation für die europäischen Marktüberwachungsbehörden bereitzuhalten und mit den Marktüberwachungsbehörden zusammenzuarbeiten.

2.2 Wer gilt unter dem CRA als Einführer oder Händler?

Für jedes Produkt mit digitalen Elementen gibt es einen Akteur, der die Rolle des Herstellers unter dem CRA innehaben wird. Dagegen kommen die Rollen des Einführers und des Händlers nicht zwangsläufig bei jedem Produkt mit digitalen Elementen zum Tragen – beispielsweise in Fällen, in denen ein Hersteller in der EU niedergelassen ist und das Produkt direkt vertreibt. Die jeweilige „Kette" an unter dem CRA verpflichteten Akteuren hängt also vom individuellen Absatzweg eines Produktes ab.

Ein **Einführer** ist gemäß Art. 3 Nr. 16 CRA eine in der Europäischen Union ansässige oder niedergelassene natürliche oder juristische Person, die ein Produkt mit digitalen Elementen auf dem Unionsmarkt in Verkehr bringt, welches den Namen oder die Marke einer natürlichen oder juristischen Person mit Sitz außerhalb der EU trägt. Die Rolle des Einführers kann für jedes Produktexemplar nur ein Akteur innehaben und sie kommt insbesondere zur Anwendung, wenn ein Produkt in einem Drittstaat produziert sowie in die Union importiert wird und der Hersteller dabei keinen Sitz innerhalb der EU hat.

Ein **Händler** ist gemäß Art. 3 Nr. 17 CRA jede natürliche oder juristische Person in der Lieferkette, die ein Produkt mit digitalen Elementen auf dem Unionsmarkt bereitstellt, dabei nicht Hersteller oder Einführer ist – und die Eigenschaften des Produkts nicht ändert. Die Rolle des Händlers kommt demnach nur in nachrangiger Weise zum Tragen, wenn der jeweilige Akteur nicht in erster Linie die Definition für Hersteller oder Einführer erfüllt.

Einführer und Händler unterliegen verschiedenen Prüfpflichten, die auf den Herstellerpflichten aufbauen.[9]

[7] Europäischen Kommission, Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 („Blue Guide"), S. 34.

[8] Europäischen Kommission, Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 („Blue Guide"), S. 38/39.

[9] Europäischen Kommission, Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 („Blue Guide"), S. 39.

2.3 Was sind „Verwalter quelloffener Software“?

Größere Open-Source-Projekte werden mitunter von Organisationen wie gemeinnützigen Vereinen getragen. Hierzu zählen bspw. die Apache Foundation, die Eclipse Foundation oder die Linux Foundation. Da **diese Einrichtungen keine kommerziellen Produkte** anbieten, aber dennoch durch die Verbreitung der dort betreuten Open-Source-Komponenten erheblichen **indirekten Einfluss** auf die Sicherheit kommerzieller Produkte ausüben, definiert der CRA eine mögliche Sonderstellung, den sogenannten „Verwalter quelloffener Software”.

Wie im Abschnitt zu Open-Source-Software (siehe A.1.5) beschrieben, werden in vielen kommerziellen Produkten Open-Source-Komponenten eingesetzt. Dadurch übertragen sich die Sicherheitsrisiken dieser Open-Source-Komponenten auf die Produkte. Viele dieser Open-Source-Projekte sind damit essenziell für sicherheitskritische Produkte. Eine Unterscheidung zwischen „quasi-geschäftlich“ betriebenen Open-Source-Projekten, zu denen große Unternehmen signifikant Ressourcen beisteuern, und kleinen Studentenprojekten ist daher notwendig, worauf im Folgenden kurz eingegangen wird.

Eine wiederkehrende Sicherheitsanalyse derselben Komponente im Rahmen jedes einzelnen Produkts mit digitalen Elementen würde den Nutzen von Open-Source-Komponenten unterminieren. Dies gilt insbesondere für die professionell und strukturiert betriebenen Projekte der OSS-Gemeinschaft.

Aus diesem Grund definiert der CRA mit den Verwaltern quelloffener Softwareine **Sonderstellung für Open-Source-Projekte**, die zwar nicht im Rahmen einer Geschäftstätigkeit bereitgestellt werden, aber nachhaltig von juristischen Personen in einem geschäftlichen Umfeld getragen werden, und die für eine Verwendung in einem kommerziellen Kontext gedacht sind (Art. 3 Nr. 14 CRA). Eine solche Intention für die Nutzung der OSS-Software in kommerziellen Produkten ist z.B. anzunehmen, wenn Entwickler kommerzieller Produkte regelmäßig und substanziell zum Open-Source-Projekt beitragen – ein solcher Beitrag muss nicht aus Entwicklungsarbeit (Code) bestehen, sondern kann z.B. auch durch finanzielle Zuwendungen (Spenden), die Bereitstellung von Software oder Hardware oder die Übernahme von Dienstleistungen (Projektmanagement, Hosting der Entwicklungsplattform, usw.) geschehen (Erwgr. 19 CRA). Eine Darstellung der Aufgaben und Pflichten der Verwalter quelloffener Software findet sich unter B.2.

3. Wo findet der CRA räumlich Anwendung?

Anknüpfungspunkt für die Anwendbarkeit der Regelungen des CRA ist gemäß Art.1 lit. a, Art. 2 Abs. 1 CRA das **Bereitstellen des Produktes mit digitalen Elementen auf dem Unionsmarkt**.

3.1 Wann gelten Produkte als auf dem Unionsmarkt bereitgestellt?

Bereitstellung auf dem (Unions-) Markt bedeutet gemäß Art. 3 Nr. 22 CRA „jede entgeltliche oder unentgeltliche Abgabe eines Produktes mit digitalen

Elementen zum Vertrieb oder zur Verwendung auf dem Unionsmarkt im Rahmen einer Geschäftstätigkeit". Die Vorschriften des CRA gelten also unabhängig davon, ob ein Produkt mit digitalen Elementen in der EU oder in einem Drittland außerhalb der EU hergestellt wurde, solange es auf dem Unionsmarkt bereitgestellt wird.

Eine Bereitstellung ist gegeben, wenn ein Angebot zum Vertrieb, wie es bereits bei einer Aufforderung zum Kauf oder bei einer Werbekampagne vorliegt, besteht und welches zu einer tatsächlichen Bereitstellung des Produktes führt. Entscheidend für die Bereitstellung auf dem Unionsmarkt ist die Endnutzung des Produktes. Soll ein Produkt letztlich außerhalb des Unionsmarktes exportiert werden, so stellt seine Lieferung, etwa zur weiteren Verarbeitung, keine Bereitstellung dar.[10]

Die Bereitstellung zielt auf jedes einzelne Produkt mit digitalen Elementen ab, nicht auf eine Produktart oder ein Produktmodell. Das bedeutet, dass *jedes einzelne* Produktexemplar bei der Bereitstellung im Unionsmarkt den geltenden Harmonisierungsvorschriften der EU entsprechen muss.[11]

Im Zusammenhang mit **Software-Produkten** knüpft die Bereitstellung mangels Körperlichkeit an die **Einräumung der Nutzungsmöglichkeit** an. Dies kann je nach Nutzungsmodell z.B. über eine Downloadmöglichkeit oder über die Übermittlung von Zugangsdaten erfolgen.[12]

3.2 Wann gelten online vertriebene Produkte als auf dem Unionsmarkt bereitgestellt?

Wenn (materielle oder immaterielle) Produkte mit digitalen Elementen **online, über Webseiten, App-Stores oder über andere online Vertriebswege** angeboten werden, stellt sich die Frage, wann hier eine „Bereitstellung auf dem Unionsmarkt" vorliegt.

Entscheidend hierbei ist, ob sich das Angebot an Nutzer in einem oder mehreren EU-Mitgliedstaaten richtet. Faktoren, die bei der Beurteilung, ob sich ein Angebot an Nutzer in der EU richtet, herangezogen werden, sind beispielweise die Sprache des Angebots, in welche Länder der Versand erfolgen kann und welche Bezahlmöglichkeiten akzeptiert werden.[13]

[10] Europäischen Kommission, Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 („Blue Guide"), S. 19.

[11] Europäischen Kommission, Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 („Blue Guide"), S. 20/21.

[12] *Wiebe; Daelen*: Der Cyber Resilience Act aus produktsicherheitsrechtlicher Perspektive, in: EuZW 2023, 257, 258.

[13] Europäischen Kommission, Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 („Blue Guide"), S. 21.

Beispiele

Wird eine Software **über eine außerhalb der EU betriebene Website als Download zum Kauf** angeboten, wobei diese Webseite auf einer primär nur in der EU gesprochenen Sprache angezeigt werden kann, ist regelmäßig ein Angebot an EU-Nutzer gegeben. Ähnlich gestaltet es sich, wenn materielle Produkte mit digitalen Elementen, wie z.B. eine Smart Watch, **physisch an Adressen innerhalb der EU versendet** werden. In diesen Fällen sind der CRA und andere EU-Harmonisierungsvorschriften durch den Hersteller einzuhalten.

Alleine die **Verfügbarkeit bzw. Abrufbarkeit einer Webseite** durch Endnutzer aus der EU reicht allerdings **nicht** aus, um von einem Angebot an EU-Nutzer auszugehen.[14] Wird z.B. auf der Webseite eines amerikanischen Herstellers eine App gegen Bezahlung zum Download angeboten, wobei die Webseite ausschließlich in englischer Sprache, der Preis in amerikanischen Dollar angegeben ist und als Bezahloption nur weltweit gängige Zahlungsdienstleister und Kreditkarten gewählt werden können, ist nicht von einem Angebot an EU-Nutzer auszugehen.

[14] Europäischen Kommission, Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 („Blue Guide"), S. 21.

B. Welche Aufgaben und Pflichten sieht der CRA für die verschiedenen Akteure vor?

Hersteller, Einführer, Händler und Verwalter quelloffener Software haben verschiedene technische, organisatorische und formale Anforderungen unter dem CRA zu erfüllen. Eine detailliertere Aufschlüsselung der Pflichten findet sich im Anhang dieses Whitepapers (siehe Anhang). Um Wirtschaftsakteuren in der Vorbereitung auf die Umsetzung des CRA einen besseren Überblick über die Bandbreite der Verpflichtungen zu ermöglichen, wurden die Verpflichtungen aus dem CRA zusammengetragen, nach Themenfeldern bzw. „Pflichtenarten" kategorisiert und tabellarisch aufbereitet. Die Tabelle kann eine anfängliche Orientierung bieten und beispielsweise bei der Planung, welche Unternehmensbereiche bei der Umsetzung einbezogen werden sollten, unterstützen. Es ist jedoch zu beachten, dass die Anforderungen des CRA hier nur grob umrissen werden und eine genaue Prüfung des Verordnungstextes erforderlich ist, sobald die finale Version hiervon vorliegt.

1. Welche Aufgaben und Pflichten sieht der CRA für Hersteller, Einführer und Händler vor?

Die Verpflichtungen des CRA richten sich **in erster Linie an die Hersteller** von Produkten mit digitalen Elementen und sind zentral in Art. 13 und 14 CRA geregelt. Eine zentrale Verpflichtung der Hersteller ist, verschiedene **Produktanforderungen** zur Cybersicherheit sowie dem **Umgang mit Schwachstellen** umzusetzen (Anhang I CRA). Hinzu kommen verschiedene **Dokumentations- und Aufbewahrungspflichten** sowie die Verpflichtung zur Durchführung eines geeigneten **Konformitätsbewertungsverfahrens**, mit dem nachzuweisen ist, dass in Bezug auf das Produkt mit digitalen Elementen die Anforderungen des CRA erfüllt sind (Art. 31 und 32 CRA). Wird dieses Konformitätsbewertungsverfahren erfolgreich abgeschlossen, haben Hersteller eine EU-Konformitätserklärung nach einem vorgegebenen Aufbau auszustellen sowie eine **CE-Kennzeichnung** auf dem jeweiligen Produkt mit digitalen Elementen anzubringen (Art. 13 Abs. 12, Art. 27 bis 30 CRA). Siehe hierzu ergänzend Info: New Legislative Framework.

Zudem treffen Hersteller verschiedene allgemeine Informations- sowie im Falle von schweren Cybersicherheitsvorfällen und aktiv ausgenutzten Schwachstellen Meldepflichten gegenüber Nutzern, Marktüberwachungsbehörden, nationalen Behörden und der ENISA. Für einen Support-Zeitraum von regelmäßig mindestens fünf Jahren haben Hersteller zudem Verpflichtungen, die die Cybersicherheit eines Produkts mit digitalen Elementen aufrechterhalten.

Die Verpflichtungen, die der CRA für **Einführer und Händler** (Art. 19 und 20 CRA) vorsieht, bauen im Wesentlichen auf den Pflichten für Hersteller auf, indem in

unterschiedlichem Umfang sicherzustellen und zu überprüfen ist, dass Hersteller CRA-Verpflichtungen in Bezug auf das jeweilige Produkt mit digitalen Elementen erfüllt haben. Zudem haben Einführer und Händler bspw. Verpflichtungen zur Zusammenarbeit mit Marktüberwachungsbehörden sowie zum Umgang mit einem Verdacht auf Nichtkonformität eines Produktes mit digitalen Elementen.

Info: New Legislative Framework

Der CRA ist an das **New Legislative Framework (NLF)** angelehnt und gliedert sich damit in die bestehende Systematik der **produktsicherheitsbezogenen EU-Harmonisierungsvorschriften** ein. Ziel des 2008 verabschiedeten Maßnahmenpakets des NLF ist die Verbesserung des Binnenmarkts für Waren und Stärkung der Bedingungen für das Inverkehrbringen von Produkten auf den EU-Markt.[15] Die Rolle der verpflichteten Wirtschaftsakteure und der Marktüberwachungsbehörden sowie verschiedene Anforderungen wie die Konformitätsbewertungsverfahren oder die CE-Kennzeichnung bauen daher auf etablierten Begriffsbestimmungen und Regulierungsmechanismen des EU-Produktsicherheitsrechts auf.[16] Auf ein Produkt mit digitalen Elementen können neben dem CRA grundsätzlich parallel auch andere Harmonisierungsvorschriften Anwendung finden (bspw. zur Sicherheit von Spielzeug, für unbemannte Luftfahrzeuge oder Messgeräte).[17] Wird die Ausstellung einer EU-Konformitätserklärung neben dem CRA bereits durch eine andere Rechtsvorschrift vorgeschrieben, können diese Erklärungen in einer gemeinsamen Konformitätserklärung abgegeben werden (Art. 28 Abs. 3 CRA). Grundsätzlich liegt es im Verantwortungsbereich der Hersteller, zu kontrollieren, ob ihre Produkte in den Anwendungsbereich einer oder mehrerer Harmonisierungsvorschriften fallen.[18]

2. Welche Aufgaben und Pflichten sieht der CRA für Verwalter quelloffener Softwarevor ?

Die **Rolle eines Verwalters quelloffener Software (siehe A.2.3) unterscheidet sich erheblich von der eines Herstellers**. So bringen Verwalter beispielsweise kein CE-Zeichen an den Open-Source-Produkten an, die sie unterstützen (Erwgr. 19 CRA). Entsprechend sind auch die Garantien, die ein Hersteller erhält, wenn er solche Open-Source-Komponenten in sein Produkt integriert, geringer als bei einer zugekauften kommerziellen Komponente, die ihrerseits dem CRA unterliegt.

[15] Europäische Kommission, New Legislative Framework, über: https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en

[16] Siehe auch hierzu den Leitfaden der Europäischen Kommission für die Umsetzung der Produktvorschriften der EU 2022 („EU Blue Guide").

[17] *Wiebe; Daelen*: Der Cyber Resilience Act aus produktsicherheitsrechtlicher Perspektive, in: EuZW 2023, 257, 259; Übersicht von Harmonisierungsvorschriften u.a. in EU Blue Guide S. 14.

[18] Europäischen Kommission, Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 („Blue Guide"), S. 17.

Rolle und Pflichten der Verwalter quelloffener Software werden in Art. 24 CRA geregelt. Zu den dort beschriebenen **Aufgaben der Verwalter quelloffener Software** gehört die Einführung und Dokumentation einer Cybersicherheits-Policy für das Open-Source-Projekt. Diese Policy soll einerseits dabei unterstützen, ein sicheres Produkt zu erzeugen (also Sicherheitslücken im Vorhinein zu vermeiden) und andererseits einen klaren Prozess festlegen, wie mit gemeldeten Sicherheitslücken verfahren wird. Sollte die Marktbeobachtungsbehörde besondere Risiken in einer Open-Source-Software erkennen, sollen die Verwalter Reduzierungen dieser Risiken unterstützen (Art. 24 Abs. 2 CRA). Diese Prozesse kommen indirekt wieder den Produktherstellern zugute, die Open-Source-Komponenten einsetzen.

Dennoch löst auch die Rolle des Verwalters das Spannungsfeld zwischen geringer reguliertem Open-Source-Umfeld und stärker regulierten Geschäftstätigkeiten nicht vollständig auf, wenn Open-Source-Komponenten in kommerzielle Produkte integriert werden. Generell erfordert der CRA eine angemessene Sorgfalt („due diligence") bei der **Integration von Drittanbieterkomponenten** in das eigene Produkt (Art. 13 Abs. 5 CRA). Soll eine kommerzielle Produktkomponente, welche entsprechend auch dem CRA unterfällt, integriert werden, kann hierfür die CRA-Pflichtdokumentation als Ausgangspunkt herangezogen werden. Ebenso kann der Integrator nach angemessener Prüfung darauf aufbauen, dass die zu integrierende Komponente die Mindestsicherheitsanforderungen erfüllt. Bei Open-Source-Produkten greifen diese Verpflichtungen zu den grundlegenden Cybersicherheitsanforderungen (Anhang I CRA) jedoch nicht. Prinzipiell müsste der Integrator diese Lücke füllen, was mit erheblichem Aufwand verbunden wäre.

Um diese Lücke zu füllen, wird die Europäische Kommission dazu ermächtigt, in Form von delegierten Rechtsakten **freiwillige „Sicherheitsbescheinigungen" (security attestation) für Open-Source-Software** zu schaffen (Art. 25 CRA). Diese können gemäß Art. 25 CRA von Entwicklern, Nutzern sowie anderen Dritten initiiert und finanziert werden und ermöglichen es, die Konformität von Open-Source-Projekten mit Anforderungen des CRA zu bewerten. So könnten Hersteller, die bereits stark zu solchen Projekten beitragen, die Sicherheitsbescheinigung für das Projekt initiieren und bezahlen (Erwgr. 21 CRA).

Dies wird vermutlich folgende Entwicklung nach sich ziehen: Die Möglichkeit des **„Sponsorings" von Sicherheitsbescheinigungen** kann zu einer Professionalisierung der Open-Source-Entwicklung führen, insbesondere für große und wichtige Projekte. Die Unternehmen profitieren von der Sicherheitsbescheinigung und tragen gleichzeitig Aufwand und Kosten. Werden Entwicklungsprozesse im Rahmen der Sicherheitsbescheinigung verbessert, kommt dies auch unabhängig von den Unternehmen wieder dem Open-Source-Projekt zugute. Gleichzeitig können zum Erhalt der Sicherheitsbescheinigung notwendige Maßnahmen die Divergenz zwischen ideell getriebenen Beitragenden und Unternehmensvertretern steigern, wenn das Kernprojekt weder zur Sicherheitsbescheinigung verpflichtet ist, noch darin einen Mehrwert gemessen an den notwendigen Änderungen sieht. Ebenso ist der Einfluss industrieller Vertreter auf die Open-Source-Projekte je nach Projekt unterschiedlich.

C. Welche Sicherheitsstufen werden bei Produkten mit digitalen Elementen unterschieden und welche Konsequenzen hat dies?

Abbildung 2: Sicherheitsstufen

Hersteller von Produkten mit digitalen Elementen müssen die Konformität mit Anforderungen des CRA mittels spezieller Verfahren nachweisen (Art. 3 Nr. 27, Art. 27 und 32 CRA). Hierbei differenziert der CRA hinsichtlich der Produkte mit digitalen Elementen und den Anforderungen an das durchzuführende Konformitätsbewertungsverfahren zwischen verschiedenen Sicherheitsstufen (siehe *Abbildung 2*). Neben der „Basiskategorie“, die für alle Produkte mit digitalen Elementen gilt, gibt es Produkte, die aufgrund ihrer Wichtigkeit bzw. Kritikalität im Rahmen des Konformitätsbewertungsverfahrens strengere Anforderungen erfüllen müssen. Die Modalitäten des durchzuführenden Verfahrens sind in Art. 27, 32 CRA geregelt, wobei dort Möglichkeiten der Standardisierung durch zukünftige harmonisierte Normen oder auch der Erwerb eines Cybersicherheitszertifikats im Sinne des Cybersecurity Acts vorgesehen sind, siehe hierzu Info: europäische Cybersicherheitszertifizierung. Abhängig von der Klassifizierung der Produkte können Hersteller das Konformitätsbewertungsverfahren bspw. selbstständig durchführen oder müssen hierfür eine externe notifizierte Stelle (Art. 3 Nr. 29 CRA) einbeziehen, siehe hierzu ergänzend Info: notifizierte Stellen.

Info: Europäische Cybersicherheitszertifizierung

Unter dem Cybersecurity Act, Verordnung (EU) 2019/881 (CSA), entwickelt die ENISA unter Beteiligung verschiedener Stakeholder europäische Schemata für die Cybersicherheitszertifizierung, die durch die Europäische Kommission mittels Durchführungsrechtsakt angenommen werden. Derzeit besteht ein entsprechendes Schema (für Produkte der Informations- und Kommunikationstechnologie), zwei weitere werden derzeit entwickelt (Cloud Services und 5G-Netzwerke).[19] In Deutschland nimmt das BSI die Rolle der im CSA festgelegten nationalen Behörde für Cybersicherheitszertifizierung (Art. 58 CSA) wahr und wird als solche u.a. auch Zertifizierungen für die Vertrauenswürdigkeitsstufe „hoch" durchführen.[20] Sind europäische Schemata zur Cybersicherheitszertifizierung in Kraft, hat die Europäische Kommission auszuweisen, dass diese zum Nachweis der Konformität mit Anforderungen des CRA verwendet werden können (Art. 27 CRA).

Info: notifizierte Stelle

Notifizierte Stellen sind von den Mitgliedstaaten nach Art. 43, 39 CRA benannte Konformitätsbewertungsstellen, also herstellerunabhängige Einrichtungen, die Aufgaben im Rahmen der Konformitätsbewertung wahrnehmen. Eine Übersicht aller unter den verschiedenen EU-Harmonisierungsvorschriften – und künftig auch dem CRA – benannten Stellen in den EU-Mitgliedsstaaten, liefert ein Informationssystem der Europäischen Kommission.[21]

Produkte mit digitalen Elementen, die einer der in Anhang III des CRA gelisteten Produktkategorien zugeordnet werden können, gelten als **„wichtige Produkte"** mit digitalen Elementen. Innerhalb dieser wichtigen Produkte wird in Anhang III CRA wiederum zwischen **Produkten der Klasse I und der Klasse II** unterschieden, wobei die Verordnung Kriterien für die Einordnung aufstellt (Art. 7 Abs. 2 CRA). Die Unterscheidung soll das mit den darunter verorteten Produktkategorien verbundene Cybersicherheitsrisiko widerspiegeln: bei Cybervorfällen im Zusammenhang mit Produkten der Klasse II ist laut Verordnungsgeber davon auszugehen, dass diese Vorfälle weitreichendere Auswirkungen haben könnten als Cybervorfälle im Zusammenhang mit Produkten der Klasse I (Erwgr. 44 CRA).

Produkte mit Sicherheitsbezug wie bspw. Passwortmanager, Browser oder „normale" Betriebssysteme für Desktops und Server fallen in **Klasse I.** In **Klasse II**

[19] Aktuelle Informationen zum Stand der EU Cybersicherheitszertifizierung durch die ENISA unter https://www.enisa.europa.eu/topics/certification/eu-cybersecurity-certification-faq/certification-schemes-and-cabs-faq?v2=1&tab=details

[20] Weitere Informationen unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/NCCA/ncca_node.html

[21] Europäische Kommission: Notified bodies (NANDO) https://webgate.ec.europa.eu/single-market-compliance-space/#/notified-bodies

fallen insbesondere Sicherheitskomponenten (Firewalls, IDS-Systeme). Zudem sind Hypervisoren erfasst. Dabei handelt es sich um die Basisbetriebssysteme virtualisierter Cloud-Plattformen. Eine Kompromittierung eines solchen Hypervisors könnte sämtliche dort betriebenen virtualisierten Clouddienste aller Kunden betreffen.

Neben den „wichtigen" Produkten, die in Anhang III CRA aufgelistet sind, sieht der CRA in Artikel 8 auch eine **Kategorie von „kritischen" Produkten** mit digitalen Elementen vor, die entsprechenden Produktkategorien werden in Anhang IV CRA gelistet. Darunter fallen Produkte wie Sicherheitsboxen oder Smartcards. Hinter dieser Regelung steht der Gedanke, dass solche Produkte im Kern **Vertrauensanker** für andere Systeme sind und somit Sicherheit der Kernaspekt des ganzen Produkts ist.

Die EU-Kommission ist gemäß Art. 7 Abs. 3 und Art. 8 Abs. 2 CRA ermächtigt, Änderungen an der Einordnung von wichtigen und kritischen Produkten vorzunehmen, z.B. neue Produktkategorien hinzuzufügen, wieder herauszunehmen oder diese in eine andere Klasse einzuordnen, wofür Übergangszeiträume von mindestens 6 bzw. 12 Monaten gelten sollen.

D. Welche Konsequenzen hat ein Verstoß gegen den CRA?

Bei Nichteinhaltung der Anforderungen des CRA drohen den verpflichteten Wirtschaftsakteuren **erhebliche Sanktionen** (siehe auch Tabelle 1). Die Mitgliedstaaten sind gemäß Art. 64 Abs. 1 CRA verpflichtet, Regelungen über wirksame, verhältnismäßige und abschreckende Sanktionen zu treffen.

Werden **unrichtige, unvollständige oder irreführende Informationen** an notifizierte Stellen oder Marktüberwachungsbehörden übermittelt, werden **Bußgelder** in Höhe von bis zu 5 Mio. EUR oder bis zu ein Prozent des weltweiten Umsatzes des vorangegangenen Geschäftsjahres verhängt (Art. 64 Abs. 4 CRA).

Darüber hinaus nennt Art. 64 Abs. 3 CRA **zahlreiche weitere Pflichten**, bei deren Verletzung ein **Bußgeld** in Höhe von bis zu 10 Mio. EUR oder bis zu zwei Prozent des weltweiten Umsatzes des vorangegangenen Geschäftsjahres verhängt werden kann. Darunter fallen unter anderem Verstöße gegen die Einführer- und Händlerpflichten (Art. 19 und 20 CRA) oder die Nichteinhaltung der Vorschriften bezüglich der Konformitätserklärung oder dem CE-Kennzeichen (Art. 28 und 30 CRA).

Bei einem **Verstoß gegen die grundlegenden Anforderungen an die Cybersicherheit**, die sich aus Anhang I ergeben, oder bei **Verstößen gegen die Herstellerpflichten** aus Art. 13 und 14 CRA, drohen nach Art. 64 Abs. 2 CRA **Bußgelder** in Höhe von bis zu 15 Mio. Euro oder bis zu 2,5 Prozent des weltweiten Umsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher Betrag höher ist.

Grund	Grundlage	Bußgelder
Auf Auskunftsverlangen hin Weitergabe von unrichtigen, unvollständigen oder irreführenden Informationen an notifizierte Stellen oder Marktüberwachungsbehörden	Art. 64 Abs. 4 CRA	bis zu 5 Mio. EUR oder bis zu 1 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher Betrag höher ist.
Verletzung der in Art. 18 bis 23, Art. 28, Art. 30 Abs. 1 bis 4, Art. 31 Abs. 1 bis 4, Art. 32 Abs. 1 bis 3, Art. 33 Abs. 5 sowie Art. 39, 41, 47, 49 und 53 CRA dargelegten Pflichten	Art. 64 Abs. 3 CRA	bis zu 10 Mio. EUR oder bis zu 2 % des weltweiten Umsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher Betrag höher ist.
Nichteinhaltung der grundlegenden Anforderungen des Anhang I oder Verstöße gegen die Herstellerpflichten aus Art. 13 und 14 CRA	Art. 64 Abs. 2 CRA	bis zu 15 Mio. Euro oder bis zu 2,5 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem, welcher Betrag höher ist.

Tabelle 1 – Verstöße und Bußgelder

Bei der Festlegung der Strafe in der Einzelfallbetrachtung sind neben der Schwere und der Dauer des Verstoßes unter anderem auch die **Größe des Unternehmens**, insbesondere bei KMUs und Start-ups, zu berücksichtigen, da diese besonders hart von hohen Strafen betroffen wären (Art. 64 Abs. 5 CRA).

Wenn Hersteller, die als **Kleinstunternehmen oder kleine Unternehmen** einzustufen sind,[22] die in Art. 14 Abs. 2 lit. a oder Abs. 4 lit. b CRA genannten Fristen der Meldepflichten nicht einhalten, sollen die oben genannten Bußgeldvorschriften gemäß Art. 64 Abs. 10 CRA keine Anwendung finden - gleiches gilt für jegliche Verstöße, die durch Verwalter quelloffener Software begangen werden.

[22] Zur Einordnung als Kleinstunternehmen sowie kleinen Unternehmen wird in Art. 3 Nr. 19 CRA auf die Empfehlung der Europäischen Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (bekannt gegeben unter Aktenzeichen K(2003) 1422) verwiesen, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32003H0361

Ausblick

Die Verabschiedung des CRA wird im Laufe des Jahres 2024 erwartet. Den verpflichteten Wirtschaftsakteuren bleibt damit eine **dreijährige Umsetzungsfrist**, innerhalb derer sie ihre Produkte und Verfahren CRA-konform gestalten müssen (Art. 71 Abs. 2 CRA). Mit Ablauf der 36 Monate werden alle Regelungen des CRA unmittelbar in jedem Mitgliedstaat gelten. Die in Art. 14 CRA geregelten Meldepflichten sollen bereits 21 Monate nach Inkrafttreten der Verordnung Anwendung finden (Art. 71 Abs. 2 CRA).

Auch wenn der Verordnungstext noch nicht final verabschiedet ist und sich viele Fragen (bspw. im Zusammenhang mit Standardisierung) erst nach Geltungsbeginn des CRA klären werden, ist es für betroffene Organisationen wichtig, sich frühzeitig mit den Regelungen des CRA zu befassen. Grundsätzlich muss Cybersicherheit in Organisationen auf der Führungsebene verankert werden und die Verantwortlichkeiten müssen klar geregelt sein. Alle Unternehmen brauchen im Themenfeld klare Zuständigkeiten, Rollen und Aufgaben – unabhängig von ihrer Größe. Es lohnt sich, anlässlich des CRA die Verankerung und Verantwortlichkeiten[23] für Cybersicherheit erneut auf den Prüfstand zu setzen, vor allem, um eventuell vorhandene Lücken zu schließen.

Grundsätzlich ist zu beachten, dass der CRA nur ein Baustein im europäischen Rechtsrahmen für Cybersicherheit ist. So kann zum Beispiel zusätzlich die **NIS2-Richtlinie** (EU) 2022/2555 für Betreiber essenzieller oder kritischer Infrastrukturen gelten. Auch das Zusammenspiel mit branchenspezifischen Regelungen, wie künftig bspw. dem Digital Operational Resilience Act (DORA) (EU) 2022/2554 im Finanzsektor, sollte von betroffenen Organisationen frühzeitig analysiert werden .

Unter https://www.athene-center.de/cra gibt es Hinweise zu Veranstaltungen, Ansprechpartnern und weitere Informationen zum CRA sowie die derzeit aktuelle Version dieses Whitepapers.

[23] Vgl. *Kreutzer; Scheel:* Smart Governance for Cybersecurity, in: ERCIM News, 2021, S. 6–7.

Anhang:
Aufgaben und Pflichten für Hersteller, Bevollmächtigte, Einführer, Händler und Verwalter quelloffener Software

Hersteller Definition in Art. 3 Nr. 13 CRA	Art. 13, 14 CRA Anhang I, II, V, VI, VII CRA

Produktanforderungen:

- Sicherstellung, dass das Produkt mit digitalen Elementen den **Sicherheitsanforderungen in Bezug auf die Eigenschaften des Produktes (Anhang I Abschnitt 1 CRA)** entspricht und nach diesen Anforderungen konzipiert, entwickelt und hergestellt worden ist
  - → z.B. Auslieferung mit einer sicheren Standardkonfiguration, Schutz vor unbefugtem Zugriff durch geeignete Kontrollmechanismen wie Authentifizierungssysteme, Verschlüsselung relevanter Daten, Datenminimierung etc.
- Sicherstellung, dass die **Anforderungen an die Behandlung von Schwachstellen** in Produkten mit digitalen Elementen (Anhang I Abschnitt 2 CRA) umgesetzt sind
- Sicherstellung, dass **von Dritten bezogene Komponenten** die Cybersicherheit des Produktes nicht beeinträchtigen

Dokumentations- und Darlegungspflichten:

- Durchführung einer **Bewertung** bzgl. der Cybersicherheitsrisiken und Minimierung entsprechender Risiken im gesamten product life cycle
  - → **Dokumentation der Risikobewertung** und regelmäßige Aktualisierung
- **Erstellung einer technischen Dokumentation** gem. Art. 31 und Anhang VII CRA
- Systematische **Dokumentation aller relevanten Cybersicherheitsaspekte**
- Durchführung eines **anwendbaren Konformitätsbewertungsverfahrens** gem. Art. 27, 32 CRA (abhängig von der Einordnung der Kritikalität/Wichtigkeit des Produktes)
- **Ausstellung einer EU-Konformitätserklärung** gem. Art. 28 CRA
- **Anbringung des CE-Kennzeichens** gem. Art. 30 CRA
- **Anbringung einer Seriennummer** oder eines anderen Elements, das der Identifizierung des Herstellers dient

Informationspflichten:

- **Beifügung der Herstellerinformationen** und **Kontaktdaten** sowie Bereitstellung eines **„single point of contact" für Nutzer**
- **Beifügung der Nutzerinformationen** gem. Anhang II CRA
- **Support-Zeitraum und -Ende** müssen bei Erwerb des Produkts leicht ersichtlich sein und, wenn möglich, Information an die Nutzer, wenn Ende des Support-Zeitraums erreicht wurde
- Bei **Einstellung der Betriebstätigkeit**, **Unterrichtung** der **Marktüberwachungsbehörden**

Aufbewahrungspflichten:

- **Aufbewahrung** der technischen Dokumentation, der Nutzerinformationen und der Konformitätserklärung für mind. zehn Jahre oder während der Dauer des Support-Zeitraums, je nachdem, welcher Zeitraum länger ist
- Auf Nachfrage der Marktüberwachungsbehörden **Übermittlung aller Informationen und Dokumentationen**, die notwendig sind, um die Konformität des Produkts nachzuweisen

Nachmarktpflichten:

- **Wirksame Schwachstellenbehandlung während des Support-Zeitraums**, der sich unter anderem an der zu erwartenden Produktlebenszeit und den Nutzererwartungen ausrichten soll
  - → Ermittlung des Support-Zeitraums (im Regelfall mindestens fünf Jahre)
  - → Schwachstellenbehandlung muss den Anforderungen des Anhangs I Abschnitt 2 CRA entsprechen
    - → z.B. Erstellung einer Software-Stückliste, Mechanismen für eine sichere Verbreitung von Aktualisierungen etc.
    - → Bereitstellung von notwendigen **Sicherheitsupdates** für Software
- Ergreifung der erforderlichen **Korrekturmaßnahmen** oder **Rücknahme bzw. Rückruf des Produkts** im Falle der Nichtkonformität während des Supportzeitraums
- **Zusammenarbeit** mit den **Marktüberwachungsbehörden**

Meldepflichten:

- **Meldung von aktiv ausgenutzten Schwachstellen und schweren Vorfällen** innerhalb von 24 Std an die nationalen CSIRTs und die ENISA sowie ggf. Information an die Nutzer des betroffenen Produktes (danach abgestuftes Meldesystem)
- Bei Feststellung einer Schwachstelle in einer integrierten Komponente **Meldung an die Person oder Einrichtung, die die Komponente wartet**

Bevollmächtigter Definition in Art. 3 Nr. 15 CRA	Art. 18 CRA

- Die Pflichten bzw. Aufgaben des Bevollmächtigten richten sich nach dem vom Hersteller erteilten schriftlichen Auftrag, wobei dieser mindestens die folgenden Aufgaben wahrnehmen können muss:
  - → **Bereithaltung der EU-Konformitätserklärung und der technischen Dokumentation** für die Marktüberwachungsbehörden für mindestens zehn Jahre oder während der Dauer des Support-Zeitraums, je nachdem, welcher Zeitraum länger ist
  - → Auf Verlangen der Marktüberwachungsbehörden Übermittlung aller erforderlichen Informationen oder Unterlagen
  - → Zusammenarbeit mit Marktüberwachungsbehörden

Einführer Definition in Art. 3 Nr. 16 CRA	Art. 19 CRA

Prüfpflichten:

- Inverkehrbringung von Produkten mit digitalen Elementen nur, wenn diese den Sicherheitsanforderungen in Bezug auf die Produkteigenschaften des Anhang I Abschnitt 1 entsprechen und wenn die vom Hersteller festgelegten Verfahren zur Schwachstellenbehandlung den Anforderungen des Anhang I Abschnitt 2 entsprechen
- Bei Anlass auf Verdacht der Nichtkonformität eines Produktes erfolgt die **Inverkehrbringung des Produktes erst dann, wenn die Konformität sichergestellt ist**
- **Sicherstellung**, dass

- → der Hersteller das geeignete Konformitätsbewertungsverfahren durchgeführt hat und die Konformitätserklärung zur Verfügung steht
- → der Hersteller die technische Dokumentation erstellt hat
- → das Produkt mit der CE-Kennzeichnung versehen ist und dass die Nutzerinformationen gem. Anhang II beigefügt sind
- → der Hersteller eine Seriennummer oder Ähnliches und seine Kontaktdaten beigefügt hat
- → das Ende des Support-Zeitraums für die Nutzer zum Erwerbszeitpunkt leicht ersichtlich ist

Informationspflichten:

- Anbringung des **Namens bzw. Handelsnamens, der Anschrift und der E-Mail-Adresse des Einführers**
- Stellt das Produkt ein **erhebliches Risiko für die Cybersicherheit** dar, unverzügliche **Information an Marktüberwachungsbehörden und Hersteller**
- Bei Feststellung einer Schwachstelle unverzügliche **Information an den Hersteller und ggf. an die entsprechenden Marktüberwachungsbehörden**, wenn das Produkt ein erhebliches Risiko für die Cybersicherheit darstellt
- Bei **Betriebseinstellung des Herstellers** Unterrichtung der Marktüberwachungsbehörden und, wenn möglich, der Nutzer

Nachmarktpflichten:

- Bei Anlass auf Verdacht der Nichtkonformität eines Produktes, das der Einführer in Verkehr gebracht hat, muss er die erforderlichen **Korrekturmaßnahmen ergreifen oder das Produkt vom Markt nehmen oder zurückrufen**
- **Zusammenarbeit** mit den **Marktüberwachungsbehörden**

Aufbewahrungspflichten:

- **Bereithaltung eines Exemplars der EU-Konformitätserklärung und der technischen Dokumentation** für mind. zehn Jahre oder während der Dauer des Support-Zeitraums, je nachdem, welcher Zeitraum länger ist
- Auf Nachfrage der Marktüberwachungsbehörden **Übermittlung aller Informationen und Dokumentationen**, die notwendig sind, um die Konformität des Produkts nachzuweisen

Händler Definition in Art. 3 Nr. 17 CRA	Art. 20 CRA

Prüfpflichten:

- Vor Bereitstellung auf dem Markt **überprüft** der Händler, dass
  - → das Produkt mit der CE-Kennzeichnung versehen ist
  - → der Hersteller die Nutzerinformationen und die EU-Konformitätserklärung dem Produkt beigefügt hat
  - → der Hersteller eine Seriennummer oder Ähnliches und seine Kontaktdaten beigefügt hat
  - → das Ende des Support-Zeitraums für den Nutzer zum Erwerbszeitpunkt leicht ersichtlich ist
  - → der Einführer dem Produkt seine Kontaktdaten beigefügt hat
- Bei Anlass auf Verdacht der Nichtkonformität des Produkts erfolgt die **Bereitstellung erst dann, wenn die Konformität sichergestellt ist**

Informationspflichten:

- Stellt das Produkt **ein erhebliches Risiko für die Cybersicherheit dar, unverzügliche Information an den Hersteller und die Marktüberwachungsbehörden**

- Bei **Feststellung einer Schwachstelle** unverzügliche **Information an den Hersteller und ggf. an die entsprechenden Marktüberwachungsbehörden**, wenn das Produkt ein erhebliches Risiko für die Cybersicherheit darstellt
- Bei **Betriebseinstellung des Herstellers** Unterrichtung der Marktüberwachungsbehörden und, wenn möglich, der Nutzer

Nachmarktpflichten:

- Bei Anlass auf Verdacht der Nichtkonformität nach Bereitstellung sorgt der Händler dafür, dass die **notwendigen Korrekturmaßnahmen getroffen werden oder das Produkt ggf. vom Markt genommen bzw. zurückgerufen wird**
- **Zusammenarbeit** mit den **Marktüberwachungsbehörden**

Aufbewahrungspflichten:

- Auf Nachfrage der Marktüberwachungsbehörden **Übermittlung aller Informationen und Dokumentationen**, die notwendig sind, um die Konformität des Produkts nachzuweisen

Verwalter quelloffener Software Definition in Art. 3 Nr. 14 CRA	Art. 24 CRA

Dokumentationspflichten:

- **Erstellung und Dokumentation einer Cybersicherheit-Policy**
  - → Förderung der Entwicklung eines sicheren Produkts mit digitalen Elementen
  - → Förderung der effektiven Schwachstellenbehandlung durch die Entwickler des Produktes
  - → Förderung der freiwilligen Meldung von Schwachstellen
- Auf Anfrage **Zusammenarbeit mit den Marktüberwachungsbehörden** und **Bereitstellung der Dokumentation der Cybersicherheits-Policy**

Meldepflichten:

- Verpflichtung **zur Meldung jeder aktiv ausgenutzten Schwachstelle** an die nationalen CSIRTs und die ENISA, abhängig davon, inwieweit der Open-Source-Software-Stewart an der Entwicklung des Produkts beteiligt ist
- Verpflichtung **zur Meldung jedes schweren Vorfalls** an die nationalen CSIRTs und die ENISA und **Information der Nutzer** über ausgenutzte Schwachstellen und schwere Vorfälle, abhängig davon, inwieweit der Vorfall sich auf Netzwerke und Informationssysteme auswirkt, die vom Open-Source-Software-Stewart bereitgestellt werden

Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik	Nationale Behörde für Cybersicherheitszertifizierung, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/NCCA/ncca_node.html [25.03.2024].
ENISA	Learn more about EU Cybersecurity Certification, https://www.enisa.europa.eu/topics/certification/eu-cybersecurity-certification-faq/certification-schemes-and-cabs-faq?v2=1&tab=details [25.03.2024].
Europäische Kommission	New legislative framework, https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en [25.03.2024].
Europäische Kommission	Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 („Blue Guide“), vom 29.6.2022.
Kreutzer, Michael; Scheel, Kirstin	Smart Governance for Cybersecurity, in: ERCIM News, 2021, S. 6-7.
Rockstroh, Sebastian	EU-Cybersicherheitsrecht für Produkte, in: Datenschutz und Datensicherheit, (DuD), 2023, Heft 6, S. 332 ff.
Wiebe, Gerhard; Daelen, Johannes	Der Cyber Resilience Act aus produktsicherheitsrechtlicher Perspektive, in: Europäische Zeitschrift für Wirtschaftsrecht (EuZW), 2023, Heft 6, S. 257 ff.

ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit