RA Stefan Hessel, LL.M. und RA Christoph Callewaert*

Der Cyber Resilience Act der EU-Kommission

Neue Herstellerpflichten zur Cybersicherheit von digitalen Produkten

Kurz und Knapp

Seit einigen Jahren hat die EU-Kommission Cybersicherheit zu einem der wichtigsten Themen für Europa auserkoren. Der kürzlich veröffentlichte Entwurf für eine Verordnung zum „Cyber Resilience Act" („CRA") soll Hersteller von digitalen Produkten zu umfassenden Maßnahmen für Cybersicherheit verpflichten. In diesem Beitrag werden die neuen Herstellerpflichten des CRA vorgestellt und in das bestehende Konzept der Produktverantwortung für Cybersicherheit eingeordnet.

I. Eine resiliente Union – die Zielsetzung des Cyber Resilience Act

1. Einleitung

„Wenn alles miteinander vernetzt ist, kann alles gehackt werden" – mit diesen Worten kündigte die EU-Kommissionspräsidentin Ursula von der Leyen in ihrer Rede zur Lage der Union am 15. 9. 2021 ein „neues Europäisches Gesetz zur Cyber-Widerstandsfähigkeit" an.[1] Auf den Tag genau ein Jahr später, am 15. 9. 2022, hat die EU-Kommission nunmehr einen Entwurf für eine entsprechende Verordnung, besser bekannt unter dem englischen Titel Cyber Resilience Act, veröffentlicht.[2] *Noch* ist nicht alles vernetzt – aber die Europäische Union, die man wegen ihrer derzeitigen Bestrebungen getrost als weltweiten Vorreiter für die Regulierung von Datenschutz, Datenwirtschaft, Künstlicher Intelligenz und Cybersicherheit bezeichnen kann, bereitet sich erkennbar auf eine umfassende Digitalisierung vor: Innerhalb weniger Jahre wurden zahlreiche neue Rechtsakte mit Bezug zur Cybersicherheit, wie z. B. der europäische Rechtsakt zur Cyber-Sicherheit („Cybersecurity Act"),[3] die delegierte Verordnung zur Radio Equipment Directive („RED"),[4] die Novelle der Richtlinie zur Sicherheit von Netz- und Informationssystemen („NIS 2")[5] sowie der Entwurf der KI-Verordnung,[6] verabschiedet oder auf den Weg gebracht. Der nun vorgelegte Entwurf für den CRA soll in diesem „Cybersicherheits-Puzzle" das vorerst letzte Teil darstellen. Durch seine horizontale Geltung soll der CRA die regulatorischen Lücken, die infolge der größtenteils vertikalen Regulierungen für einzelne Bereiche und Produkte noch verbleiben, schließen und die bestehenden Regelungen verbinden.

2. Ursachen und Folgen von Cyberangriffen

Dass mehr Cybersicherheit notwendig ist, zeigt bereits ein Blick in den Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI): Allein in Deutschland konnte mit 144 Mio. neuen Schadprogrammvarianten eine Zunahme von 22 % gegenüber dem Vorjahreszeitraum verzeichnet werden.[7] Dies deckt sich mit den europäischen Zahlen: Nach Angaben der EU-Kommission findet alle elf Sekunden ein Ransomware-Angriff, also eine Verschlüsselung von Daten mit anschließender Lösegeldforderung, statt.[8] Ransomware-Angriffe haben im vergangenen Jahr Schäden bzw. Kosten in Höhe von 20 Milliarden Euro verursacht.[9] Weltweit entstanden im Jahr 2021 infolge von Cyberkriminalität geschätzte Kosten in Höhe von über 5,5 Billionen Euro.[10]

Die Gründe für diese gravierenden Auswirkungen von Cyberangriffen sind nach Auffassung der EU-Kommission auch in einem generell niedrigen Cybersicherheitsniveau von digitalen Produkten begründet. Bestehende Sicherheitsrisiken würden zudem durch weit verbreitete Sicherheitslücken sowie eine unzureichende und inkonsistente Bereitstellung von Sicherheitsupdates vergrößert.[11] Außerdem soll auch ein unzureichendes Verständnis von Cyberrisiken sowie ein unzureichender Zugang zu Informationen zur aktuellen Cybersicherheitslage für die Missstände verantwortlich sein. Beides hindere Nutzer daran, Produkte mit angemessenen Cybersicherheitseigenschaften auszuwählen oder die Produkte auf sichere Weise zu nutzen.[12]

Die EU-Kommission schätzt die Cyberrisiken für den europäischen Binnenmarkt als verheerend ein: In einer vernetzten Umgebung könne ein Cybersicherheitsvorfall

* Mehr über die Autoren erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 28. 9. 2022.

1 Abrufbar unter https://ec.europa.eu/info/sites/default/files/soteu_2021_address_de_0.pdf.

2 Abrufbar unter https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

3 Abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32019R0881.

4 Abrufbar unter https://single-market-economy.ec.europa.eu/system/files/2021-10/C_2021_7672_F1_COMMISSION_DELEGATED_REGULATION_EN_V10_P1_1428769.PDF.

5 Siehe zum letzten Stand https://data.consilium.europa.eu/doc/document/ST-10193-2022-INIT/x/pdf.

6 Abrufbar unter https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

7 Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland, 2021, S. 42, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf?__blob=publicationFile&v=4.

8 EU-Kommission, Cyber Resilience Act – Factsheet, abrufbar unter https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet.

9 EU-Kommission, Cyber Resilience Act – Factsheet, abrufbar unter https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet.

10 EU-Kommission, Cyber Resilience Act – Factsheet, abrufbar unter https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet.

11 Cyber Resilience Act, ErwG 1.

12 Cyber Resilience Act, ErwG 1.

in einem einzelnen Produkt ein ganzes Unternehmen oder eine ganze Lieferkette betreffen und sich binnen weniger Minuten über die Grenzen des Binnenmarkts hinweg verbreiten, was wiederum zu einer schwerwiegenden Unterbrechung wirtschaftlicher und sozialer Aktivitäten führen oder sogar lebensbedrohlich werden könne.[13] Gerade mit Blick auf Lieferketten stellt die EU-Kommission fest, dass deren Sicherheit nur gewährleistet sei, wenn *alle* in ihr enthaltenen Komponenten geschützt seien.[14] In Bezug auf die Lieferkettensicherheit hatte zuletzt auch die europäische Cybersicherheitsagentur ENISA Abwehrmaßnahmen und Empfehlungen veröffentlicht und unter anderem zu einer Identifizierung von Lieferanten- und Softwareabhängigkeiten sowie „Single Points of Failure" und entsprechenden vertraglichen Regelungen geraten.[15] Die Cybersicherheit von Lieferketten gilt nicht zuletzt deshalb als mögliches Feld für weitere, bisher nicht angekündigte, Regulierungen durch die EU-Kommission.

3. Ziele des CRA

Mit dem CRA verfolgt die EU-Kommission das übergeordnete Ziel, die EU gegen Cyberangriffe und Sicherheitsvorfälle resilienter zu machen. Hierzu soll ein horizontaler Rechtsrahmen geschaffen werden, der umfassende Cybersicherheitsanforderungen für alle digitalen Produkte festlegt.[16] Konkret soll der CRA hierfür vier spezifische Ziele erreichen: Der CRA soll (i) dafür sorgen, dass Hersteller die Cybersicherheit von digitalen Produkten bereits in der Design- und Entwicklungsphase berücksichtigen und während des gesamten Lebenszyklus aufrecht erhalten; (ii) einen kohärenten Rahmen für Cybersicherheit schaffen, der die Einhaltung der Vorschriften für Hardware- und Softwarehersteller erleichtert; (iii) die Transparenz der Cybersicherheit von digitalen Produkten verbessern und (iv) Unternehmen und Verbraucher in die Lage versetzen, digitale Produkte sicher zu nutzen.[17] Zugleich – dies betont die EU-Kommission ausdrücklich – sollen die Vorgaben des CRA auch Rechtssicherheit für Hersteller schaffen.[18] Der CRA soll nicht zu einer Behinderung für Innovationen und die Bereitstellung von Produkten auf dem europäischen Markt führen.

4. Aufbau und Systematik des CRA

Der Entwurf des CRA ist in acht Kapitel gegliedert und in insgesamt 57 Artikel unterteilt. Während Kapitel I neben allgemeinen Vorgaben insbesondere den Anwendungsbereich der Verordnung und die darin enthaltenen Begrifflichkeiten definiert, enthält Kapitel II konkrete Vorgaben für Hersteller sowie weitere Marktakteure. In Kapitel III und IV wird die Konformitätsbewertung von Produkten und in Kapitel V die Marktüberwachung inklusive deren Durchsetzung erläutert. Für den Fall der Missachtung der Vorgaben des CRA hält Kapitel VII Sanktionsmöglichkeiten, unter anderem in Form von Bußgeldern, bereit.

II. Die Vorgaben des CRA im Überblick

1. Anwendungsbereich und erfasste Produkte

Der CRA ist anwendbar auf Produkte mit digitalen Elementen bzw. digitale Produkte („product with digital elements"). Ein Produkt mit digitalen Elementen ist „jedes Software- oder Hardwareprodukt und seine Ferndatenverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die separat in Verkehr gebracht werden sollen." Unter „Software" ist gem. Art. 3 Abs. 6 CRA der Teil eines elektronischen Informationssystems, der aus Computercode besteht zu verstehen. „Hardware" meint nach Art. 3 Abs. 7 CRA ein physisches elektronisches Informationssystem, welches digitale Daten verarbeiten, speichern oder übertragen kann, oder einen Teil davon. Aus diesen äußerst weit gefassten Definitionen folgt ein breiter Anwendungsbereich des CRA, der einen breiten Schutz vor Cyberrisiken von digitalen Produkten bewirken soll.

Daneben kennt der CRA auch „critical products with digital elements", also kritische Produkte mit digitalen Elementen. Die Produkte, die hiervon erfasst werden, sind in Annex III des CRA aufgelistet und in zwei Klassen („Class I" und „Class II") unterteilt, wobei die in Class II aufgelisteten Produkte ein höheres Risiko mit sich bringen.[19] Während unter Class I beispielsweise Passwortmanager, Netzwerkmanagementsysteme oder physische Netzwerkschnittstellen aufgelistet werden, finden sich in Class II unter anderem Betriebssysteme für Desktop- oder Mobilgeräte, Mikroprozessoren und Smartcards sowie deren Lesegeräte.

2. Ausnahmen vom Anwendungsbereich

Trotz oder gerade aufgrund des sehr weiten Anwendungsbereichs werden über Art. 2 CRA bestimmte, zumeist sektorspezifische, digitale Produkte ausgenommen. Der CRA findet gem. Art. 2 Abs. 2 CRA beispielsweise keine Anwendung auf Medizinprodukte („Medical Devices Regulation")[20] oder In-vitro-Diagnostika („IVDR").[21] Grundsätzlich von der Anwendbarkeit ausgenommen werden sollen nach Art. 2 Abs. 5 CRA darüber hinaus Produkte mit digitalen Elementen, die exklusiv für die nationale Sicherheit, militärische Zwecke oder speziell zur Verarbeitung vertraulicher Informationen konzipiert wurden. Zudem kann die Geltung des CRA gem. Art. 2 Abs. 4 CRA für digitale Produkte, die unter andere Vorschriften der EU fallen, eingeschränkt oder ganz ausgeschlossen werden, wenn ein solcher Ausschluss mit dem für diese Produkte geltenden allgemeinen Rechtsrahmen vereinbar ist und die jeweiligen sektoralen Vorschriften das gleiche Schutzniveau erreichen. In ihrem Entwurf gewährt sich die EU-Kommission hierbei das Recht, die betroffenen Produkte und Vorschriften über nachträgliche delegierte Rechtsakte zum CRA zu bestimmen.

Das aufgrund des breiten Anwendungsbereichs des CRA unklare Verhältnis zu anderen (zukünftigen) Rechtsakten der EU, wie z. B. der allgemeinen Produktsicherheitsverordnung, der KI-Verordnung und der Maschinenverordnung, wird in den Art. 7 ff. CRA adressiert.[22] Im Kern legen die Bestimmungen des CRA insoweit zumindest in Bezug auf bestimmte Eigenschaften oder Teile der Produkte eine ergänzende Geltung der genannten Rechtsakte

13 Cyber Resilience Act, Einleitung, S. 1.
14 Cyber Resilience Act, Einleitung, S. 2.
15 ENISA, ENISA Threat Landscape for Supply Chain Attacks, July 2021, S. 27 f., abrufbar unter: https://www.enisa.europa.eu/publications/threat landscape-for-supply-chain-attacks; Siehe hierzu auch *Hessel/Potel/Beerwald*, K&R 2021, 773 f.
16 Cyber Resilience Act, ErwG 4.
17 Cyber Resilience Act, Einleitung, S. 1.
18 Cyber Resilience Act, ErwG 4.
19 Cyber Resilience Act, Einleitung, S. 10.
20 VO (EU) 2017/745, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32017R0745.
21 VO (EU) 2017/746, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv:OJ.L_.2017117.1.0176.01.DEU&toc=OJ:L:2017:117:TOC.
22 Siehe hierzu auch den Abschnitt „Interplay with other Union policies", Cyber Resilience Act, Einleitung, S. 3.

bzw. eine in Teilen wechselseitige Anerkennung der Konformität entsprechend der jeweiligen Vorschriften fest.

Eine besondere Rolle spielen hierbei die Funkanlagenrichtlinie („Radio Equipment Directive")[23] sowie die delegierte Verordnung der EU-Kommission zur Funkanlagenrichtlinie vom 29. 10. 2021:[24] Aufgrund des weiten Anwendungsbereichs gilt der CRA für alle Funkanlagen, die in den Anwendungsbereich der delegierten Verordnung fallen und enthält zudem sämtliche in Art. 3 Abs. 3 lit. d, e und f der Funkanlagenrichtlinie aufgezählten grundlegenden Anforderungen.[25] Um regulatorische Überschneidungen zu vermeiden, ist nach Angaben der EU-Kommission vorgesehen, die delegierte Verordnung in Bezug auf die von dem CRA erfassten Funkanlagen aufzuheben oder zu ändern, sodass für diese ausschließlich der CRA Anwendung finden soll.[26]

3. Neue Vorgaben für Hersteller, Importeure und Händler

a) Produktvorgaben und Meldepflichten für Hersteller

aa) Der Herstellerbegriff nach dem CRA

Die Adressaten des CRA sind in erster Linie die Hersteller von digitalen Produkten („manufacturer"). Hierdurch setzt sich der CRA insbesondere von der europäischen Datenschutz-Grundverordnung (DSGVO) ab, welche sich in erster Linie an die für die Datenverarbeitung Verantwortlichen richtet und mithin die Hersteller datenverarbeitender Produkte allenfalls mittelbar adressiert, wie Erwägungsgrund 78 der DSGVO bestätigt: Danach sollen Hersteller lediglich „ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen".[27]

Was unter einem Hersteller im Sinne des CRA zu verstehen ist, wird in Art. 3 Abs. 18 CRA definiert: Ein Hersteller ist jede natürliche oder juristische Person, die digitale Produkte entwickelt oder herstellt. Ausdrücklich erfasst werden auch natürliche oder juristische Personen, die digitale Produkte entwerfen, entwickeln oder herstellen lassen und diese unter ihrem Namen oder ihrer Marke vertreiben. Dieser weite Adressatenkreis ist Ausdruck der mit dem CRA verfolgten Strategie einer größtmöglichen Cybersicherheit von digitalen Produkten.

bb) Compliance mit den Vorgaben des CRA

Die Vorgaben für Hersteller sind in Art. 10 CRA in insgesamt 15 Absätzen geregelt. Erste und zentrale Vorgabe für Hersteller ist es gem. Art. 10 Abs. 1 CRA, sicherzustellen, dass das jeweilige Produkt in Übereinstimmung mit den grundlegenden Anforderungen an digitale Produkte entworfen, entwickelt und hergestellt wird. Die grundlegenden Anforderungen sind in Abschnitt 1 des Annex I zum CRA zu finden. Unter der Überschrift „Sicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen" werden die Grundsteine für die Cybersicherheit nach dem CRA gelegt. Gemäß Abschnitt 1 Abs. 1 müssen Produkte ganz allgemein so entworfen, entwickelt und herstellt werden, dass sie – mit Blick auf die jeweiligen Risiken – ein angemessenes Maß an Cybersicherheit gewährleisten. Hierzu gehört, wie Abs. 2 betont, dass die Produkte ohne bekannte ausnutzbare Schwachstellen geliefert werden müssen. Konkretisiert werden diese allgemeinen Vorgaben in Abs. 3, welcher unter anderem die Auslieferung mit einer sicheren Standardkonfiguration, die Möglichkeit der Zurücksetzung in den ursprünglichen Zustand, geeignete Kontrollmechanismen zum Schutz vor unbefugtem Zugriff oder eine Minimierung von Daten verlangt. Zudem sollen die Produkte dergestalt entworfen, entwickelt und produziert werden, dass die Auswirkungen eines Vorfalls reduziert werden und zugleich sichergestellt werden kann, dass Schwachstellen durch (ggf. automatische) Sicherheitsupdates behoben werden können.

cc) Durchführung einer Risikobewertung

Nach Art. 10 Abs. 2 CRA sollen Hersteller zukünftig verpflichtet sein, eine Bewertung der Cybersicherheitsrisiken ihres digitalen Produkts durchzuführen und das Ergebnis in der Planungs-, Entwurfs-, Entwicklungs-, Produktions-, Liefer- und Wartungsphase zu berücksichtigen. Die Risikobewertung ist gem. Art. 23 CRA in die technischen Unterlagen aufzunehmen. Art. 10 Abs. 5 CRA verpflichtet die Hersteller zu einer kontinuierlichen und systematischen Dokumentation der Cybersicherheitsrisiken des digitalen Produkts. Die Pflicht zur fortlaufenden Produktüberwachung wird auch in Art. 10 Abs. 6 CRA aufgegriffen. Hersteller sollen dazu verpflichtet werden für die erwartete Lebensdauer des jeweiligen Produkts, mindestens aber für fünf Jahre – je nachdem welches der kürzere Zeitraum ist – sicherzustellen, dass erkannte Schwachstellen des Produkts wirksam geschlossen werden. Näheres regelt Abschnitt 2 des Annex I. Darin werden Hersteller unter anderem dazu verpflichtet, effektive und regelmäßige Tests und Überprüfungen der Sicherheit des Produkts durchzuführen und Schwachstellen unverzüglich, „auch durch die Bereitstellung von Sicherheitsupdates", zu beheben. Weshalb der vorgegebene Zeitraum auf fünf Jahre beschränkt wurde, bleibt mit Blick auf die teilweise deutlich längere Lebensdauer von digitalen Produkten unklar.

dd) Responsible Disclosure und Cybersicherheit von Lieferketten

Für die Bereitstellung der Sicherheitsupdates sollen die Hersteller dazu verpflichtet werden, eine Übersicht der im Produkt verwendeten Softwarekomponenten in einem allgemein gebräuchlichen und maschinenlesbaren Format zu führen. Dies soll gerade mit Blick auf die Nutzung von standardisierten Softwarekomponenten, die in einer Vielzahl von digitalen Produkten[28] genutzt werden, einen entscheidenden Beitrag zur Cybersicherheit leisten: Denn nur wenn der Hersteller weiß, welche Komponenten in seinem Produkt zum Einsatz kommen, kann er präventiv auf Sicherheitslücken sowie reaktiv auf Sicherheitsvorfälle reagieren und betroffene Marktteilnehmer und Nutzer informieren.

Darüber hinaus sollen Hersteller koordinierte Richtlinien zur Offenlegung von Sicherheitslücken einführen. Mit diesen soll die Meldung von Sicherheitslücken erleichtert und so eine Untersuchung und Behebung von Sicherheitslücken ermöglicht werden.[29] Da Informationen über Sicherheitslücken teils zu hohen Preisen auf dem Schwarzmarkt verkauft werden, sollen Hersteller über (finanzielle)

23 RL 2014/53/EU, abrufbar unter https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0053.
24 Abrufbar unter https://single-market-economy.ec.europa.eu/system/files/2021-10/C_2021_7672_F1_COMMISSION_DELEGATED_REGULATION_EN_V10_P1_1428769.PDF.
25 Cyber Resilience Act, Einleitung, S. 3.
26 Cyber Resilience Act, Einleitung, S. 3.
27 Datenschutz-Grundverordnung, ErwG 78.
28 *Wonnemann*, Datenschutz und Datensicherheit, 2022, S. 455.
29 Cyber Resilience Act, ErwG 36.

Entschädigungen Anreize für die verantwortungsvolle Meldung von Sicherheitslücken schaffen und dementsprechende „Bug Bounty Programme“ einführen.[30]

ee) Informationspflichten gegenüber Verbrauchern

Nach Art. 10 Abs. 10 CRA sollen Hersteller sicherstellen, dass den Produkten die in Annex II des CRA aufgezählten Informationen und Anleitungen klar, nachvollziehbar und in einer für den Benutzer leicht verständlichen Sprache in elektronischer oder physischer Form beigefügt sind. Darunter fallen neben den Kontaktdaten des Herstellers sowie einer Kontaktstelle, bei der Informationen über Cybersicherheitsschwachstellen des Produkts gemeldet werden können, auch Angaben zur Identifizierung des jeweiligen Produkts.

ff) Meldepflicht gegenüber der ENISA

Durch Art. 11 CRA werden Herstellern insbesondere im Fall von Sicherheitslücken umfassende Meldepflichten auferlegt. Die erste und wichtigste Pflicht zur Meldung findet sich in Art. 11 Abs. 1 CRA: Danach müssen Hersteller der europäischen Cybersicherheitsagentur ENISA jede aktiv ausgenutzte Schwachstelle in einem von ihnen hergestellten digitalen Produkt unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntniserlangung melden. Die Meldung soll Details zu der Schwachstelle sowie Informationen zu etwaigen getroffenen Abhilfemaßnahmen enthalten. Erkennbar soll die ENISA durch die Meldepflicht in die Lage versetzt werden, schnell ein Lagebild zu möglichen Sicherheitsrisiken erstellen zu können, um weitere relevante Behörden informieren und gegebenenfalls koordinierte Maßnahmen ergreifen zu können. In Ausnahmefällen soll die ENISA auf Ersuchen der Kommission in der Lage sein, Bewertungen von digitalen Produkten durchzuführen, die ein erhebliches Cybersicherheitsrisiko darstellen und bei denen ein sofortiges Eingreifen erforderlich ist, um das reibungslose Funktionieren des Binnenmarktes zu gewährleisten.[31]

Neben einer Meldepflicht für aktiv ausgenutzte Schwachstellen, verpflichtet Art. 11 Abs. 2 CRA die Hersteller auch zur Meldung von anderen Vorfällen, die Auswirkungen auf die Sicherheit des digitalen Produkts haben. Bezüglich dieser Meldepflichten behält sich die EU-Kommission in Art. 11 Abs. 5 CRA die Möglichkeit vor, delegierte Rechtsakte zu erlassen, welche die Art der Informationen, das Format und das jeweilige Meldeverfahren näher bestimmen. Die EU-Kommission misst den Meldepflichten offenkundig eine wesentliche Bedeutung zu und es ist davon auszugehen, dass der Meldeprozess bei Bedarf über delegierte Rechtsakte verschärft werden wird.

Betroffene Nutzer sollen gem. Art. 11 Abs. 4 CRA nach Bekanntwerden eines Vorfalls ebenfalls unverzüglich über den Vorfall sowie über etwaige Abhilfemaßnahmen, die der Nutzer ergreifen kann, informiert werden. Darüber hinaus müssen Hersteller gem. Art. 11 Abs. 7 CRA bei einer Schwachstelle in einer (Open-Source-)Komponente die Person oder Einrichtung, welche die Komponente wartet, informieren.

b) Vorgaben für weitere Marktakteure

aa) Importeure und Händler

Auch wenn sich die Vorgaben des CRA in erster Linie an Hersteller richten, enthält der Entwurf des CRA auch Vorgaben für Importeure (Art. 13 CRA) und Händler (Art. 14 CRA). Unter dem Importeur ist nach der Legaldefinition in Art. 3 Abs. 20 CRA jede in der EU ansässige natürliche oder juristische Person zu verstehen, die ein digitales Produkt in Verkehr bringt, welches den Namen oder die Marke einer außerhalb der EU ansässigen natürlichen oder juristischen Person trägt. Ein Händler ist gem. Art. 3 Abs. 21 CRA jede natürliche oder juristische Person in der Lieferkette, die nicht der Hersteller oder der Importeur ist und die ein digitales Produkt auf dem Binnenmarkt bereitstellt, ohne dessen Eigenschaften zu verändern. Sofern der Importeur oder Händler ein Produkt unter seinem Namen oder seiner Marke in Verkehr bringt bzw. wesentliche Änderungen an einem bereits in Verkehr gebrachten Produkt vornimmt, gilt er gem. Art. 15 CRA selbst als Hersteller und hat die entsprechenden Herstellerpflichten zu beachten.

bb) Vorgaben für Importeure

Importeure sollen gem. Art. 13 Abs. 1 CRA grundsätzlich nur digitale Produkte in Verkehr bringen, die den oben erläuterten Anforderungen an die Cybersicherheit entsprechen. Den Importeur trifft dabei die Pflicht zu kontrollieren, ob der Hersteller seine Pflichten in Bezug auf das importierte Produkt eingehalten hat. Der Importeur soll vor dem Inverkehrbringen insbesondere sicherstellen, dass der Hersteller die einschlägigen Konformitätsbewertungsverfahren gem. Art. 24 CRA durchgeführt, die technischen Dokumente erstellt und das europäische CE-Kennzeichen in korrekter Form und inklusive der erforderlichen Instruktionen angebracht hat. Bei Nichtkonformität eines Produkts ist der Importeur dazu verpflichtet, die Konformität entweder selbst herzustellen oder das entsprechende Produkt im Zweifel nicht in Verkehr zu bringen.

Neben diesen Kontrollpflichten treffen Importeure nach Art. 13 Abs. 6 ff. CRA im Fall der Nichtkonformität des importierten Produkts umfassende Melde- und Informationspflichten gegenüber dem Hersteller sowie der zuständigen Marktüberwachungsbehörde. Diese, sowie die Nutzer, hat der Importeur gem. Art. 13 Abs. 9 CRA auch zu informieren, wenn er davon Kenntnis erlangt, dass der Hersteller den Betrieb eingestellt hat und somit seine Pflichten nach dem CRA nicht mehr erfüllen kann.

cc) Vorgaben für Händler

Den Händler wiederum treffen gem. Art. 14 Abs. 2 CRA ebenfalls bestimmte Kontrollpflichten in Bezug auf die in Art. 14 Abs. 2 lit. b CRA genannten Vorgaben für Hersteller und Importeure, wie die Beifügung der in Annex II genannten Informationen oder der Konformitätserklärung. Zudem ist der Händler im Falle der Bereitstellung eines Produkts mit digitalen Elementen auf dem Markt nach Art. 14 Abs. 1 CRA zu einem Handeln „mit der gebotenen Sorgfalt in Bezug auf die Anforderungen dieser Verordnung“ verpflichtet. Insgesamt orientieren sich die Vorschriften für Händler jedoch – teilweise in abgeschwächter Form – an den Vorgaben für Importeure, sodass auf diese nicht in detaillierter Form eingegangen werden soll.

III. Konformitätsbewertung

Das Konformitätsbewertungsverfahren ist in den Kapiteln III und IV geregelt. Aufgrund der zahlreichen bereits auf den Weg gebrachten Rechtsakte findet sich in Art. 18 CRA

30 Cyber Resilience Act, ErwG 36.
31 Cyber Resilience Act, ErwG 19.

zunächst eine Vermutungsregelung: Nach dieser gilt im Falle einer Konformität des Produkts mit den Vorgaben bestimmter anderer Rechtsakte eine Vermutung der Konformität in Bezug auf die in Annex I des CRA genannten grundlegenden Vorgaben. Besonders hervorzuheben ist die Regelung des Art. 18 Abs. 3 CRA: Danach greift eine Konformitätsvermutung, wenn das Produkt nach dem Cybersecurity Act zertifiziert ist. Das bisherige Konzept der freiwilligen Zertifizierung wird also nicht völlig bedeutungslos. Es ist allerdings dennoch davon auszugehen, dass der CRA die Konzepte zur freiwilligen Zertifizierung mittel- bis langfristig ablösen wird.

Die eigentlichen Vorgaben zur Konformitätsbewertung nach dem CRA finden sich in den Art. 20 ff. CRA, die wiederum durch ergänzende und konkretisierende Angaben in den Annexen IV, V und VI flankiert werden. In Annex IV sind eine Reihe von Angaben enthalten, welche die EU-Konformitätserklärung zwingend enthalten muss, wie unter anderem die Kontaktdaten des Herstellers oder die Erklärung, dass der Gegenstand der beschriebenen Erklärung im Einklang mit den einschlägigen Harmonisierungsvorschriften der EU steht. In vergleichbarer Weise enthalten Annex V, zur nach Art. 23 CRA erforderlichen technischen Dokumentation, und Annex VI, in Bezug auf das in Form von Modulen in Art. 24 CRA geregelte Verfahren der Konformitätsbewertung, ebenfalls zwingend zu beachtende Vorgaben.

IV. Marktüberwachung und Durchsetzung

Aufgrund der umfassenden Vorgaben und der großen Reichweite der Bestimmungen des CRA dürfte eine der zentralen Herausforderungen die Umsetzung und Rechtsdurchsetzung der jeweiligen Vorschriften sein. Dies scheint auch der EU-Kommission bewusst. Der Überwachung und Durchsetzung der Vorgaben des CRA wird in den Art. 41 ff. CRA ein eigenes Kapitel gewidmet.

1. Zuständige Behörde

Nach Art. 41 Abs. 2 CRA soll jeder Mitgliedstaat eine für die Überwachung und Durchsetzung zuständige Behörde benennen. Die EU-Kommission betont, dass die Mitgliedstaaten sowohl eine bestehende als auch eine neue Behörde für die Marktüberwachung benennen können. Mit Blick auf dessen bereits bestehende Aufgaben ist davon auszugehen, dass die entsprechenden Marktüberwachungsaufgaben in Deutschland durch das BSI übernommen werden. Auch eine Zuständigkeit der Bundesnetzagentur (BNetzA) oder ggf. eine Kooperation mit dieser erscheint denkbar. Eine Ausnahme besteht nach Art. 41 Abs. 10 CRA für als Hochrisiko-KI eingestufte künstliche Intelligenz nach der zukünftigen KI-Verordnung: Hier soll die bereits nach der KI-Verordnung zuständige Behörde auch Marktüberwachungsbehörde für die Einhaltung der Vorgaben des CRA sein.

Jede nationale Marktüberwachungsbehörde soll gem. Art. 41 Abs. 3 CRA mit den Zertifizierungsstellen nach dem Cybersecurity Act kooperieren. Da diese Aufgabe in Deutschland dem BSI zufällt, würden bei einer erwarteten Zuständigkeit des BSI nach dem CRA beide Aufgaben in ein Haus fallen. Zudem soll die Marktüberwachungsbehörde nach dem CRA gem. Art. 41 Abs. 4 CRA mit anderen, aufgrund von harmonisierten Vorschriften festgelegten Marktüberwachungsbehörden, sowie gem. Art. 41 Abs. 5 CRA mit den jeweiligen nationalen Datenschutzaufsichtsbehörden zusammenarbeiten. Letzteres erscheint mit Blick auf die bei Cybersicherheitsvorfällen häufig betroffenen personenbezogenen Daten und die in Art. 33, 34 DSGVO vorgesehenen Melde- und Benachrichtigungspflichten durchaus sinnvoll. Die Datenschutzaufsichtsbehörden erhalten nach Art. 41 Abs. 5 CRA darüber hinaus auf Anfrage Zugang zu der nach dem CRA erforderlichen Dokumentation. In diesem Zusammenhang dürfte es interessant zu beobachten sein, ob anhand dieser Informationen die aus rechtlicher Sicht zumindest fragwürdige Praxis einzelner Datenschutzaufsichtsbehörden, Produkte abstrakt auf ihre Vereinbarkeit mit datenschutzrechtlichen Vorschriften zu bewerten und ggf. Warnungen auszusprechen,[32] zunehmen wird.

Ebenfalls interessant ist im Hinblick auf die Datenschutzaufsichtsbehörden die Regelung des Art. 41 Abs. 6 CRA, wonach die Mitgliedstaaten sicherstellen müssen, dass die benannten Marktüberwachungsbehörden mit angemessenen finanziellen und personellen Ressourcen ausgestattet werden, um die ihnen nach dem CRA obliegenden Aufgaben erfüllen zu können. Ob dies dazu führt, dass die strengen Vorgaben „auf dem Papier“ auch in der Praxis durchgesetzt werden können, bleibt jedoch abzuwarten.

2. Marktmaßnahmen

Die Maßnahmen der Marktaufsichtsbehörden sind in Art. 43 CRA geregelt. Hat eine Behörde den begründeten Verdacht, dass ein digitales Produkt den Anforderungen des CRA nicht entspricht, kann sie nach Art. 43 Abs. 1 CRA eine Untersuchung einleiten. Stellt die Marktüberwachungsbehörde im Rahmen der Untersuchung fest, dass Anforderungen nicht erfüllt werden, soll sie das betreffende Unternehmen unverzüglich auffordern, Korrekturmaßnahmen zu ergreifen, um die Konformität wiederherzustellen. Darüber hinaus kann die zuständige Behörde auch die Entfernung des digitalen Produkts vom Markt bzw. einen Rückruf innerhalb einer angemessenen Frist verlangen. Ist die nationale Behörde der Auffassung, dass sich die Nichtkonformität nicht auf ihren Zuständigkeitsbereich beschränkt, so ist sie zur Unterrichtung der EU-Kommission und der übrigen Mitgliedstaaten verpflichtet. Die Unterrichtung soll sowohl Informationen zu den Ergebnissen der Bewertung als auch zu ggf. bereits getroffenen Maßnahmen enthalten. Unabhängig davon können die Marktüberwachungsbehörden der Mitgliedstaaten unter den Voraussetzungen des Art. 48 CRA gemeinsame Aktivitäten zur Gewährleistung der Cybersicherheit und des Schutzes der Verbraucher sowie nach Art. 49 CRA koordinierte Kontrollmaßnahmen, sogenannte „Sweeps“, durchführen.

Gelingt dem Hersteller die Umsetzung der angeordneten Maßnahmen innerhalb eines angemessenen Zeitraums nicht, kann die Marktüberwachungsbehörde die entsprechenden Maßnahmen gem. Art. 43 Abs. 4 CRA auch selbst vornehmen. Schließlich sieht Art. 53 CRA für den Fall der Nichtkonformität – in Anlehnung an das Bußgeldkonzept der DSGVO – die Verhängung von Bußgeldern in Höhe von bis zu 15 Mio. Euro bzw. 2,5 % des weltweiten Jahresumsatzes des vergangenen Jahres vor, je nachdem welcher Betrag höher ist.

V. Auswirkungen auf die Praxis

Der geplante CRA stellt eine deutliche Verschärfung der rechtlichen Anforderungen an die Cybersicherheit von

32 *Hessel/Schneider*, K&R 2022, 82 ff.

digitalen Produkten und den damit einhergehenden Pflichten dar. Auch wenn sich die Vorgaben in erster Linie an Hersteller richten, müssen sich auch Importeure und Händler auf einen erheblichen Mehraufwand durch Überprüfungspflichten einstellen. Unternehmen sollten daher frühzeitig prüfen, ob und inwieweit sie vom CRA betroffen sind und rechtzeitig Maßnahmen zur Umsetzung vornehmen. Hierzu gehört insbesondere auch die Implementierung eines geschützten Kanals für Sicherheitsupdates. Updatability kann auch bei der zunehmenden Zahl von Produktwarnungen durch staatliche Stellen, wie dem BSI[33] aber auch den Datenschutzaufsichtsbehörden[34] einen entscheidenden Einwand in Bezug auf die Verhältnismäßigkeit der jeweiligen Warnung darstellen und die Erfolgsaussichten der (gerichtlichen) Überprüfung erhöhen. Darüber hinaus sollten betroffene Unternehmen einen an die Vorgaben des CRA angepassten internen Prozess zum Umgang mit Sicherheitslücken und Produktwarnungen definieren. Dieser sollte unter anderem festlegen, welche Fachabteilung im Ernstfall einzubeziehen ist und welche Behörden ggf. innerhalb welcher Fristen zu informieren sind.

VI. Fazit

Aus Sicht der EU-Kommission stellt der CRA den vorerst letzten Schlussstein der europäischen Produktvorgaben dar. Für eine belastbare Aussage, ob damit sprichwörtlich „das Beste zum Schluss" kommt, ist es in dem aktuellen Entwurfsstadium jedoch noch zu früh. Bereits jetzt ist jedoch festzuhalten, dass der CRA viele gute Ansätze enthält und die EU-Kommission über den weiten Anwendungsbereich erkennbar eine größtmögliche Cybersicherheit von Produkten anstrebt. Gleichzeitig stellt der CRA eine weitere Belastung für – mit Blick auf die vielfältigen und zuletzt umfassend verschärften Vorgaben für Cybersicherheit – ohnehin schon „belasteten" Unternehmen dar. Nunmehr werden sich zunächst das EU-Parlament und der Europäische Rat mit dem Entwurf der EU-Kommission befassen. Nach einer Einigung der Institutionen und der Veröffentlichung im Amtsblatt der EU wird der CRA dann mit Übergangsfristen von 12 bzw. 24 Monaten in Kraft treten. Mit Blick auf die bereits heute bestehenden rechtlichen Risiken bei unzureichender Cybersicherheit von digitalen Produkten sollten Unternehmen dies jedoch nicht zum Anlass nehmen, das Thema auf die lange Bank zu schieben, sondern ein produktbezogenes Cybersecurity Compliance Management aufbauen.

33 Siehe hierzu die Warnung des BSI vor dem Einsatz von Kaspersky-Virenschutzprodukten, abrufbar unter https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html; Vgl. auch OVG NRW, 28. 4. 2022 – 4 B 473/22, K&R 2022, 555 ff. = MMR 2022, 695 ff.; Erst kürzlich warnte das BSI zudem vor dem Einsatz unsicherer Funk-Türschlösser der Marke ABUS, abrufbar unter https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220810_Warnung_ABUS.html.

34 Siehe für einen Überblick *Hessel/Schneider*, K&R 2022, 82 ff.

Stefan Hessel
ist Salary Partner und Head of Digital Business bei reuschlaw Legal Consultants in Saarbrücken.

Christoph Callewaert
ist Associate bei reuschlaw Legal Consultants in Saarbrücken.

RA Dr. Florian Deusch und Prof. Dr. Tobias Eggendorfer*

Update IT-Sicherheitsrecht 2021/2022

Kurz und Knapp

Die Autoren stellen anschließend an ihr Update aus dem Vorjahr in K&R 2021, 689 ff. die Entwicklung des IT-Sicherheitsrechts im Zeitraum 2021/22 anhand ausgewählter Akte der Gesetzgebung und der Rechtsprechung sowie Stellungnahmen aus der Verwaltung dar.

I. Einführung und Gefährdungslage

Durch ausgenutzte („exploits") Sicherheitslücken bzw. Schwachstellen („vulnerabilities") können sich Bedrohungen („threats") als Angriffe („attacks") auf IT-Systeme realisieren, die die Ziele der IT-Sicherheit (insbesondere Verfügbarkeit, Vertraulichkeit, Authentizität und Integrität) beeinträchtigen. Je nach Angriff fallen IT-Systeme teilweise oder vollständig aus, werden von nicht autorisierten Tätern überwacht oder sogar ferngesteuert, exfiltrieren unberechtigt Daten an Dritte oder arbeiten sonstig nicht mehr funktionsgerecht.[1] Die European Cybersecurity Agency (ENISA), das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Polizeibehörden beschreiben im Berichtszeitraum dazu folgende Gefährdungslage:[2]

* Der Beitrag geht auf einen Vortrag der Autoren bei der DSRI-Herbstakademie 2022 zurück, der veröffentlicht wurde im Tagungsband von Heinze (Hrsg.), Daten, Plattformen und KI als Dreiklang unserer Zeit, 2022, S. 803 ff. Er ist überarbeitet und aktualisiert zum Stand Oktober 2022. Alle zitierten Internetquellen wurden zuletzt abgerufen am 11. 10. 2022. Mehr über die Autoren erfahren Sie am Ende des Beitrags.

1 Zum technischen Hintergrund: *Sohr/Kemmerich*, in: Kipker (Hrsg.), Cybersecurity, 2020, Kap. 2 Rn. 1 - 14, 155 - 189; *Deusch/Eggendorfer*, in: Taeger/Pohle (Hrsg.), Computerrechts-Handbuch, 37. Ergänzung, 2022, Kap. 50.1 Rn. 6 - 26, 31 - 169.

2 ENISA, Threat Landscape 2021 (https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 mit den gelisteten Major Incidents im Annex), BSI Lagebericht 2021 (https://www.bmi.bund.de/SharedDocs/