Kommunikation & Recht

K&R

2 | Februar 2025
28. Jahrgang
Seiten 73-144

dfv Mediengruppe
Frankfurt am Main

schen Schrifttum, sondern auch mit den Marktüberwachungsbehörden und vor Gerichten. Die Wirtschaftsakteure sollten sich intensiv mit diesen Herausforderungen beschäftigen. Es ist davon auszugehen, dass sich die Marktüberwachungsbehörden insbesondere in der Anfangsphase auf die Einhaltung der weniger umstrittenen Pflichten konzentrieren werden. Es wird bspw. vergleichsweise einfach sein, einen Rückruf daraufhin zu bewerten, ob die Formalien eingehalten und Abhilfemaßnahmen angeboten wurden, oder ob bei nicht-harmonisierten Produkten die elektronische Adresse auf dem Produkt angegeben ist. Es wäre wünschenswert, wenn die EU, die Zentralstelle der Länder für Sicherheitstechnik („ZLS“) und der Länderausschuss für Arbeitsschutz und Sicherheitstechnik („LASI“) schnell Handreichungen erarbeiten würden, die den Wirtschaftsakteuren eine verlässlichere Bereitstellung ihrer Verbraucherprodukte ermöglichen.

Dr. Ulrich Becker

Studium an der Universität Jena; Referendariat in Frankfurt a. M. und London; seit 2007 zugelassener Anwalt und seit 2017 Partner in der Kanzlei CMS Deutschland in Frankfurt a. M.; Head of CMS Practice Group Product Compliance; Schwerpunktbereiche: Produktsicherheits- und Produkthaftungsrecht und Vertriebsrecht; regelmäßiger Referent zu diesen Themen.

Sinje Maier

Studium an der Universität Freiburg und an der Universität Grenoble, Frankreich; Referendariat in Frankfurt a. M. und Miami, USA; seit 2015 zugelassene Anwältin und seit 2019 Anwältin und Counsel in der Kanzlei CMS Deutschland in Frankfurt a. M.; Schwerpunktbereiche: Produktsicherheits- und Produkthaftungsrecht und Vertriebsrecht; Referentin zu diesen Themen.

RA Dr. Gerhard Wiebe, Johannes Daelen, LL.M. und Benjamin Kerger, B. Eng.*

Der neue Cyber Resilience Act

Regulierung der produktbezogenen Cybersicherheit

Kurz und Knapp

Die am 10. 12. 2024 in Kraft getretene VO (EU) 2024/2847 legt erstmals verbindliche Cybersicherheitsanforderungen für eine Vielzahl von Produkten mit digitalen Elementen für den gesamten Produktlebenszyklus fest. Mit diesem neuen Rechtsakt kreiert die EU einen Grundpfeiler bei der Regulierung der produktbezogenen Cybersicherheit und der Digitalisierung von Produkten, den es lohnt, näher in den Blick zu nehmen.

I. Einführung

Mit der zunehmenden Digitalisierung und Vernetzung von Produkten hat sich auch die Zahl der Cyberangriffe in den letzten Jahren deutlich erhöht. Weltweit verursachen Cyberangriffe jedes Jahr Kosten in Höhe von 5,5 Bio. EUR.[1] Täglich werden weltweit über 2200 Cyberangriffe registriert, was einem Angriff alle 39 Sekunden entspricht.[2] Verantwortlich für diese Angriffe sind sowohl staatlich unterstützte Akteure und organisierte Cyberkriminelle als auch Einzelpersonen, die Schwachstellen in IT-Systemen ausnutzen.[3] Cyberangriffe werden häufig durch Phishing, das Versenden manipulativer E-Mails zur Erlangung vertraulicher Informationen, sowie durch den Einsatz von Malware wie Ransomware oder Trojanern durchgeführt. Weitere gängige Methoden umfassen Denial-of-Service – (DoS)-Angriffe, bei denen Systeme durch gezielte Überlastung lahmgelegt werden, und Exploits, die Sicherheitslücken in Software oder Netzwerken ausnutzen. Diese Techniken zielen oft darauf ab, Zugang zu sensiblen Daten zu erhalten, IT-Infrastrukturen zu stören oder Lösegeldforderungen durchzusetzen.

Cyberangriffe beeinträchtigen nicht nur die Funktionsfähigkeit des Staates und die Wirtschaft als solche, sondern wirken sich im produktbezogenen Kontext u. a. auch auf die Datensicherheit sowie den -schutz aus und können sogar die Sicherheit und Gesundheit der Nutzer negativ betreffen.[4] Produktbezogene Cyberangriffe und die von ihnen ausgehenden Risiken lassen sich laut der Kommission u. a. auf zwei Hauptprobleme zurückführen: Einerseits sind sog. Produkte mit digitalen Elementen nicht ausreichend gegen böswillige Angriffe geschützt, andererseits sind die Nutzer von Produkten mit digitalen Elementen häufig nicht ausreichend darüber informiert, wie sie ein sicheres Produkt auswählen oder verwenden können.[5]

Vor diesem Risikohintergrund formt die am 20. 11. 2024 im EU-Amtsblatt veröffentlichte Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (sog. Cyberresilienz-Verordnung oder Cyber Resilience Act, im Folgenden „CRA“)[6] Rahmenbedingungen für die Entwicklung und das Inverkehrbringen cybersicherer Produkte mit digitalen Elementen. Einem technologieneutralen, risikobasierten *security by design*-Ansatz folgend zielt der CRA darauf ab, die Entwicklung cybersicherer Produkte mit digitalen Elementen zu fördern, ohne dabei Innovationsräume unnötig einzuschränken. Als Regelungskonzept liegt dem CRA das sog. New Legislative Framework (NLF) zugrunde.[7] Der CRA verfasst folglich eine horizontale Harmonisierungsrechtsvorschrift bzw. einen sog. CE-Rechtsakt, der eine Vielzahl unterschiedlicher Schutzziele vereint.

* Mehr über die Autoren erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 7. 1. 2024.

1 *Wiebe/Daelen*, EuZW 2023, 257; *Dittrich/Heinelt*, RDi 2023, 309, 310.

2 https://securityboulevard.com/2023/11/how-many-cyber-attacks-happen-per-day-in-2023/.

3 https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2024.

4 Erwägungsgrund 1; *Wiebe*, InTeR 2021, 66, 67.

5 *Dittrich/Heinelt*, RDi 2023, 309, 310.

6 ABl. L, 2024/2847, 20. 11. 2024.

7 *Wiebe/Daelen*, EuZW 2023, 257, 258.

In Anlehnung an die NLF-Struktur skizziert der Beitrag zunächst den Anwendungsbereich des CRA (II.) sowie dessen Ziele und die geschützten Rechtsgüter (III.). Darauf aufbauend werden die Produktanforderungen (IV.), die Pflichten der Wirtschaftsakteure (V.) sowie die Regelungen zur Durchsetzung des CRA (VI.) ausführlich dargestellt. Abschließend folgen ein Fazit und ein Blick nach vorne (VII.).

II. Anwendungsbereich

1. Sachlicher Anwendungsbereich: Produkte mit digitalen Elementen

Art. 2 Abs. 1 CRA eröffnet den sachlichen Anwendungsbereich für auf dem Markt bereitgestellte *Produkte mit digitalen Elementen*. Ein Produkt mit digitalen Elementen ist gem. Art. 3 Abs. 1 CRA „ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in den Verkehr gebracht werden". Daraus ergibt sich eine entsprechend weite Definition des Begriffs „Produkte mit digitalen Elementen", unter die grundsätzlich jegliche Soft- und Hardware fällt, sofern sie digitale Daten verarbeiten, speichern oder übertragen kann. Exemplarisch unterfallen dem CRA Betriebssysteme, Apps, intelligente Maschinen (IIoT[8]) und IoT-Verbraucherprodukte wie vernetzte Haushaltsgeräte mit Sicherheitsfunktionen, inklusive intelligenter Türschlösser, Babyphone-Systemen und Alarmanlagen, vernetztes Spielzeug und am Körper tragbare medizinische Geräte (Wearables).[9]

Eine besondere Rolle ist für freie und quelloffene Software (sog. free and open source software, FOSS) vorgesehen. Freie und quelloffene Software ist „eine Software, deren Quellcode offen geteilt wird und die im Rahmen einer kostenlosen Open-Source-Lizenz zur Verfügung gestellt wird, die alle Rechte vorsieht, um sie frei zugänglich, nutzbar, veränderbar und weiterverteilbar zu machen" (Art. 3 Nr. 48 CRA). FOSS soll grundsätzlich nur dann in den Anwendungsbereich des CRA fallen, wenn sie zum Vertrieb oder im Rahmen einer Geschäftstätigkeit verfügbar gemacht wird – entscheidend ist, ob die Software „zu Geld gemacht wird" bzw. ob sie einen „kommerziellen Charakter" aufweist.[10] Die Abgrenzung zwischen kommerziellen und nicht kommerziellen Charakter wird die Praxis vor Schwierigkeiten stellen.

Cloud-Computing-Dienste sowie entsprechende Dienstleistungsmodelle wie Software-as-a-Service und webbasierte Anwendungen sind vom Anwendungsbereich des CRA ausgenommen.[11] Gleiches gilt für Medizinprodukte i. S. d. VO (EU) 2017/745 bzw. VO (EU) 2017/746 sowie Automotive-Produkte, die unter die VO (EU) 2019/2144 fallen (Art. 2 Abs. 2 CRA). Praktische Bedeutung hat zudem die Ausnahme nach Art. 2 Abs. 6 CRA, wonach der CRA sich nicht auf Ersatzteile erstreckt, die identische Komponenten in Produkten mit digitalen Elementen ersetzen, sofern sie nach denselben Spezifikationen hergestellt werden wie die zu ersetzenden Bauteile.

2. Persönlicher Anwendungsbereich

In persönlicher Hinsicht verpflichtet der CRA die klassischen Wirtschaftsakteure gem. Art. 3 Nr. 12 CRA, zu denen Hersteller i. S. v. Art. 3 Nr. 13 CRA, Bevollmächtigte des Herstellers i. S. v. Art. 3 Nr. 15 CRA, Einführer i. S. v. Art. 3 Nr. 16 CRA und Händler i. S. v. Art. 3 Nr. 17 CRA rechnen. Zu den Wirtschaftsakteuren zählt darüber hinaus „jede andere natürliche oder juristische Person, die Verpflichtungen im Zusammenhang mit der Herstellung von Produkten mit digitalen Elementen oder der Bereitstellung auf dem Markt von Produkten mit digitalen Elementen im Einklang mit dieser Verordnung unterliegt" (Art. 3 Nr. 12 CRA). Verwalter quelloffener Software, für die sich Pflichten aus Art. 24 CRA ergeben, gehören hingegen nicht zum Kreis der Wirtschaftsakteure. Bei diesem handelt es sich um eine juristische Person, die – ohne Hersteller zu sein – „den Zweck oder das Ziel hat, die Entwicklung spezifischer Produkte mit digitalen Elementen, die als freie und quelloffene Software gelten und für kommerzielle Tätigkeiten bestimmt sind, systematisch und nachhaltig zu unterstützen, und die die Brauchbarkeit dieser Produkte sicherstellt" (Art. 3 Nr. 14 CRA).

3. Tätigkeitsbezogener Anwendungsbereich

Die Pflichten der Wirtschaftsakteure knüpfen an das Inverkehrbringen bzw. die Bereitstellung auf dem Markt an (Art. 2 Abs. 1 CRA). Letzterer Begriff meint gem. Art. 3 Nr. 22 CRA „die entgeltliche oder unentgeltliche Abgabe eines Produkts mit digitalen Elementen zum Vertrieb oder zur Verwendung auf dem Unionsmarkt im Rahmen einer Geschäftstätigkeit". Nach h. M. erfordert die Abgabe eines Produkts einen Übergang der tatsächlichen Sachherrschaft,[12] der bei Hardware und der dort integrierten Software ohne Weiteres möglich ist. Der faktische Sachherrschaftswechsel setzt eine physische Greifbarkeit des Produkts voraus, an der es zumindest bei Stand-alone-Software mangelt. Da in diesem Fall ein Anknüpfungspunkt für den Wechsel der Sachherrschaft fehlt, muss die Produktabgabe an die Einräumung der Nutzungsmöglichkeit gekoppelt werden.[13] Die Modalitäten dieser Nutzungseinräumung variieren je nach Nutzungsmodell. Sie kann durch Zurverfügungstellen der Installationsdateien, beispielsweise mittels Downloadoption, oder durch die Übermittlung von Zugangsdaten bzw. die Freischaltung des Nutzers erfolgen.[14]

4. Zusammenspiel mit anderen EU-Produktrechtsvorschriften

Der CRA hat eine horizontale Geltungsrichtung.[15] Etwas kryptisch ordnet Art. 2 Abs. 5 S. 1 CRA den Vorrang von sektoralen Harmonisierungsrechtsvorschriften mit spezifischen Cybersicherheitsanforderungen an, wenn dies mit dem für die betroffenen Produkte geltenden allgemeinen Rechtsrahmen vereinbar ist. Zudem müssen die anwendbaren sektorspezifischen Vorschriften zumindest dasselbe Schutzniveau wie der CRA erreichen. Diese Konkurrenzregel spiegelt den Charakter des CRA als „Allgemeiner Teil" des produktbezogenen Cybersicherheitsrechts und als mindestschutzgewährendes Auffangnetz wider.

Auf das Verhältnis zu drei in praxi wichtigen Regelungskreisen geht der CRA genauer ein: Erstens genießen die sicherheitsrelevanten Harmonisierungsrechtsvorschriften bzw. die VO (EU) 2023/988 (sog. EU-Produktsicherheitsverordnung – GPSR) Vorrang in Bezug auf die Produktsicherheit (im Sinne von Safety), vgl. Art. 11 CRA. Die GPSR und der CRA können daher unter Umständen parallele Anwendung finden, wenn keine vorrangige safety-relevante Harmonisierungsrechtsvor-

8 Industrial Internet of Things.
9 Erwägungsgrund 9.
10 Erwägungsgrund 18; vgl. speziell mit Blick auf freie und quelloffene Software *Schöttle*, ZfPC 2023, 215; *Dittrich/Heinelt*, RDi 2023, 309, 311.
11 Erwägungsgrund 12, vgl. *Dittrich/Heinelt*, RDi 2023, 309, 311.
12 *Klindt/Schucht*, in: Klindt, ProdSG, 3. Aufl. 2021, § 2 Rn. 26 ff.; *Schucht/Wiebe*, Die neue EU-Produktsicherheitsverordnung, 2024, § 3 Rn. 43.
13 *Wiebe/Daelen*, EuZW 2023, 257, 258.
14 Ebenso aus Sicht des Produkthaftungsrechts *Wagner*, in: MüKo BGB, 9. Aufl. 2024, § 2 ProdHaftG, Rn. 23 ff.
15 Erwägungsgrund 28.

schrift greift.[16] Zweitens gelten die KI-rechtlichen Anforderungen an die Cybersicherheit nach Art. 15 VO (EU) 2024/1689 (sog. KI-Verordnung) als erfüllt, wenn das Hochrisiko-KI-System den Vorgaben des CRA entspricht (Art. 12 CRA). Drittens müssen Produkte, die sowohl in den Anwendungsbereich des CRA als auch in den der VO (EU) 2023/1230 (sog. EU-Maschinenverordnung) fallen, den Vorgaben beider Rechtsakte genügen. Sofern sich bestimmte grundlegende Anforderungen überschneiden, können mit der Einhaltung der Anforderungen des CRA auch die cybersicherheitsbezogenen Vorgaben in den Nrn. 1.1.9 und 1.2.1 des Anhangs III der VO (EU) 2023/1230 erfüllt werden. Dies muss der Hersteller allerdings nachweisen können, z. B. durch die Anwendung harmonisierter Normen (vgl. Erwägungsgrund 53 zum CRA).

III. Ziele und Schutzgüter

Die Zielrichtung des CRA bezieht sich auf die Gewährleistung eines hohen Niveaus an Cybersicherheit (Art. 1 lit. a CRA);[17] die Anforderungen des CRA sollen die Widerstandsfähigkeit von Produkten vor Cyberangriffen während des gesamten Lebenszyklus sicherstellen. Beim Herausschälen des Inhalts und der Rechtsgüter der Cybersicherheit (die mitunter mit der IT-Sicherheit gleichgesetzt werden)[18] hilft die Begriffsbestimmung gem. Art. 3 Nr. 3 CRA i. V. m. Art. 2 Nr. 1 VO (EU) 2019/88 nur bedingt. Danach bezeichnet die „Cybersicherheit" „alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen".

Bei Lichte betrachtet bezweckt der CRA a priori den Schutz der Vertraulichkeit, Authentizität, Integrität und Verfügbarkeit personenbezogener und sonstiger Daten, wie nicht zuletzt die Anforderungen in Anhang I verdeutlichen.[19] Der Begriff „Authentizität" bezeichnet die Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit einer Einheit. In diesem Zusammenhang ist auch die Nichtabstreitbarkeit als Schutzziel zu erwähnen; darunter ist die Fähigkeit zu verstehen, beweisen zu können, dass eine Handlung zwischen zwei Parteien stattgefunden hat (und keine Wiederholung zulässt). Im Übrigen hat die Autorisierung eine hohe Relevanz; dies ist die Eigenschaft, nur privilegierten Nutzern den Zugang zu Bereichen eines Systems zu gewähren.[20] Zugleich zielt der CRA auf die Sicherstellung der Funktionsfähigkeit von Netz- und Informationssystemen. Aus grundrechtlicher Sicht stehen damit der Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme sowie der informationellen Selbstbestimmung im Zentrum (Artt. 2 Abs. 1 i. V. m. 1 Abs. 1 GG). Indem eine verbesserte Cybersicherheit auch vor Produktbeeinträchtigungen und -manipulationen bewahrt, trägt der CRA ebenso dem Eigentumsschutz bei.[21]

Obgleich das Hauptaugenmerk des CRA auf der Gewährleistung der Cybersicherheit im Sinne von „Security" (Schutz von Produkten vor Menschen) liegt, dient er zumindest mittelbar ebenfalls der Produktsicherheit im Sinne von Safety (Schutz von Menschen vor Produkten, indem diese vor anderen Menschen geschützt werden), wie Art. 13 Abs. 2 CRA indiziert.[22] Schließlich können Produktmanipulationen unter Ausnutzung von IT-Sicherheitslücken zu Gefahren für die Sicherheit und Gesundheit von Personen führen.[23] IT-Sicherheitslücken begründen latente Gefahren für die Personensicherheit.[24] Dies gilt umso mehr, als Nutzer sich gegen Cyberangriffe nur schlecht verteidigen können, da der Zugriff auf Produkte mit digitalen Elementen aufgrund ihrer Konnektivität einfacher ist als bei analogen Produkten und Hacker anonym, unbemerkt und aus der Distanz agieren.[25]

IV. Anforderungen an Produkte mit digitalen Elementen

1. Formelle Produktanforderungen

Die formellen Produktanforderungen des CRA bilden Voraussetzungen für die Verkehrsfähigkeit eines Produkts. Ein Verstoß gegen diese nicht-cybersicherheitsrelevanten Vorgaben löst gleichwohl nur eine minderschwere sog. formelle Nichtkonformität aus (vgl. Art. 58 CRA). Die Anordnung einschneidender marktüberwachungsbehördlicher Korrekturmaßnahmen – wie z. B. Rückrufe – ist in diesen Fällen aus Verhältnismäßigkeitserwägungen in der Regel nicht zulässig.[26]

Eine zentrale formelle Anforderung besteht in der Ausstellung der EU-Konformitätserklärung durch den Hersteller (Art. 28 Abs. 1 CRA). Mit der EU-Konformitätserklärung, die dem Produkt beizufügen ist (Art. 13 Abs. 20 CRA), übernimmt der Hersteller gem. Art. 28 Abs. 4 CRA die Verantwortung für die Konformität des Produkts und erklärt die Einhaltung der grundlegenden Cybersicherheitsanforderungen nach Anhang I des CRA. Eine Qualitätsaussage bzw. objektive Konformitätsbestätigung geht damit ebenso wenig wie mit der Anbringung der CE-Kennzeichnung gem. Art. 30 Abs. 1 CRA einher. Beide typische NLF-Instrumente spiegeln den erfolgreichen Abschluss des Konformitätsbewertungsverfahrens wider, dienen darüber hinaus aber nicht als unwiderlegbarer Nachweis, sondern allenfalls als Indiz für die tatsächliche Konformität.[27] Die CE-Kennzeichnung ist gut sichtbar, leserlich und dauerhaft auf dem Produkt anzubringen. Handelt es sich bei dem Produkt um unverkörperte Software, so ist gem. Art. 30 Abs. 1 S. 3 CRA die CE-Kennzeichnung entweder in der Konformitätserklärung oder auf der begleitenden Website des Softwareprodukts anzugeben.

Daneben müssen Produkte mit digitalen Elementen mit Identifikations-, Hersteller- und Einführerangaben gekennzeichnet werden. Die Identifikationskennzeichnung umfasst gem. Art. 13 Abs. 15 CRA die Typen-, Chargen- oder Seriennummer oder ein anderes Kennzeichen zur eindeutigen Produktidentifikation (zwecks Rückverfolgbarkeit). Die Herstellerkennzeichnung besteht aus dem Namen bzw. der Marke, der Postanschrift, der E-Mail-Adresse oder anderer digitaler Kontaktangaben des Herstellers sowie, soweit vorhanden, der Website, unter der der Hersteller zu erreichen ist (Art. 13 Abs. 16 CRA). Inhaltlich gleichlaufend regelt Art. 19 Abs. 4 CRA die Kennzeichnung des Einführers. Die genannten Kennzeichnungen gilt es, vorrangig auf dem Produkt selbst anzubringen. Ausnahmsweise – etwa bei technischer Unmöglichkeit der produktunmittelbaren Kennzeichnung – darf auf die Begleitunterlagen oder die Verpackung ausgewichen werden; bei eigenständiger Software dürften sich digitale Begleitunterlagen als Anbringungsort anbieten.

16 Erwägungsgrund 50.
17 Erwägungsgrund 11.
18 Vgl. § 2 Abs. 2 S. 3 BSIG.
19 Erwägungsgrund 32.
20 Vgl. Anhang A der EN 18031-1:2024.
21 *Wiebe/Daelen*, EuZW 2023, 257, 258.
22 *Wiebe/Daelen*, EuZW 2023, 257, 258; *Wiebe*, ZRP 2023, 73 f.
23 Erwägungsgrund 43.
24 *Wiebe*, in: Schucht/Wiebe, GPSR, 2024, Art. 6 Rn. 33.
25 *Wiebe*, ZRP 2023, 73, 74.
26 *Wiebe/Daelen*, EuZW 2023, 257, 258.
27 Vgl. *Wilrich*, Das neue Produktsicherheitsgesetz, 2012, Rn. 469 f.; *Schumann*, Bauelemente des europ. Produktsicherheitsrechts, 2007, S. 135; *Wiebe*, Unternehmerfreiheit versus Verbraucherschutz?!, 2017, S. 324 f.; *Wende*, in: Klindt, ProdSG, 3. Aufl. 2021, § 7 Rn. 6; Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 („Blue Guide"), hrsg. v. der Europäischen Kommission, 2022, Abschnitt 4.5.1.1.

2. Materielle Produktanforderungen

Die materiellen (d. h. cybersicherheitsrelevanten) Vorgaben setzen sich zusammen aus den in Anhang I Teil I verankerten grundlegenden Cybersicherheitsanforderungen (a.), deren Detailausgestaltung technischen Regelwerken überlassen wird (b.), und den instruktiven Anforderungen (c.). Eine materielle Nichtkonformität begründet fehlende Verkehrsfähigkeit und zieht regelmäßig schärfere rechtliche Folgen nach sich als bei einem Verstoß gegen formelle Anforderungen.

a) Konstruktive bzw. entwicklungsbezogene Anforderungen

Ein Produkt mit digitalen Elementen darf gem. Art. 6 Abs. 1 CRA nur dann auf dem Markt bereitgestellt werden, wenn es den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I des CRA genügt. Die einzuhaltenden Anforderungen sind nach Art. 6 Abs. 1 i. V. m. Anhang I Teil I Abs. 1 des CRA in Abhängigkeit von den zu ermittelnden Cybersicherheitsrisiken (dazu unter V. 1. b.) zu identifizieren, die von dem Produkt ausgehen. Folglich müssen diese Anforderungen nicht bei jedem Produkt eins-zu-eins umgesetzt werden, zumal dies faktisch selten möglich sein wird. Die Anforderungen zielen nicht auf den vollständigen Ausschluss von Cyberrisiken ab; schließlich ist eine absolute Cybersicherheit de facto nicht zu erreichen.[28] Sie vereinen anerkannte Prinzipien und Best Practices aus der Softwareentwicklung und betreffen die Konzipierung, Entwicklung und Konstruktion. Exemplarisch sollen einige Anforderungen näher betrachtet werden:

- Das Produkt darf nicht mit bekannten, ausnutzbaren Schwachstellen auf dem Markt bereitgestellt werden (Anhang I Teil I Abs. 2 lit. a CRA). Öffentlich bekannte Sicherheitslücken und andere Schwachstellen in Computersystemen (sog. Common Vulnerabilities and Exposures, CVE) werden in einer Datenbank gepflegt.[29] Um die Ausnutzbarkeit von Schwachstellen im Produktkontext bewerten zu können, ist es ggf. ratsam, zusätzliche Metriken heranzuziehen, um die Ausnutzbarkeit zu bewerten.[30] Lässt sich beispielsweise eine Schwachstelle nur durch den physischen Zugriff auf ein Produkt ausnutzen, wird der Score niedriger sein, als wenn sich die Schwachstelle auch aus dem Internet ausnutzen lässt.
- Das Produkt muss mit einer sicheren Standardkonfiguration auf dem Markt bereitgestellt werden (*security by default*, Anhang I Teil I Abs. 2 lit. b CRA).
- Schwachstellen müssen durch Sicherheitsaktualisierungen behoben werden können (Anhang I Teil I Abs. 2 lit. c CRA).[31] Dabei gilt es jedoch, zu beachten, dass nicht jedes Produkt mit digitalen Elementen die notwendigen Eigenschaften für das Einspielen einer Sicherheitsaktualisierung vorweisen kann. Ein Flusssensor, ein Fensterkontaktsensor oder ein elektronischer Schalter sind etwa womöglich in ihren Eigenschaften eingeschränkt; Einschränkungen im Bereich der Energieversorgung, des Datenspeichers, der Prozessorleistung und der Ausgestaltung von Kommunikationsschnittstellen sind hier denkbar, die ein Softwareupdate unmöglich machen. Wenn eine Sicherheitsaktualisierung nicht möglich ist, kann eine Strategie für einen physischen Produktaustausch bzw. eine physische Nachrüstung geboten sein.[32]
- Schutz vor unbefugtem Zugriff durch Identifikations- und Authentifizierungssysteme (Anhang I Teil I Abs. 2 lit. d CRA).
- Schutz der Vertraulichkeit von Daten durch Verschlüsselung (Anhang I Teil I Abs. 2 lit. e CRA).
- Schutz der Integrität von Daten (Anhang I Teil I Abs. 2 lit. f CRA). Daten dürfen nicht manipuliert oder verändert werden, wenn dies nicht vom Nutzer beabsichtigt ist. Von dem Begriff „Daten" umfasst sind nicht etwa nur personenbezogene Daten i. S. d. der VO (EU) 2016/679, sondern darüber hinaus auch Anweisungen an das Programm, die Programme selbst und gespeicherte Konfigurationen.
- Begrenzung der Datenerfassung auf ein erforderliches Maß (Anhang I Teil I Abs. 2 lit. g CRA).
- Das Produkt muss über wesentliche und grundlegende Funktionen verfügen. Diese müssen auch nach einem Sicherheitsvorfall zur Verfügung stehen. Hiervon erfasst sein müssen Abwehr- und Eindämmungsmaßnahmen gegen Überlastungsangriffe auf Server (Denial-of-Service-Angriffe, vgl. Anhang I Teil I Abs. 2 lit. h CRA). So muss z. B. der smarte Kühlschrank seine wesentliche Funktion – das Kühlen von Lebensmitteln – auch während Verbindungsproblemen zum Server verrichten können.
- Vermeidung negativer Auswirkungen auf die Verfügbarkeit der von anderen Geräten oder Netzen bereitgestellten Dienste (Anhang I Teil I Abs. 2 lit. i CRA).
- Das Produkt muss so konzipiert, entwickelt und hergestellt sein, dass es eine möglichst geringe Angriffsfläche bietet, indem potenzielle Schwachstellen und Sicherheitslücken minimiert werden (Anhang I Teil I Abs. 2 lit. j CRA).
- Fähigkeit, die Auswirkungen eines Sicherheitsvorfalls durch geeignete Mechanismen und Techniken zur Minderung der möglichen Ausnutzung zu verringern (Anhang I Teil I Abs. 2 lit. k CRA).
- Das Produkt muss die Fähigkeit haben, sicherheitsbezogene Aktivitäten in Softwareanwendungen und -systemen aufzuzeichnen und zu überwachen (Anhang I Teil I Abs. 2 lit. l CRA).
- Das Produkt muss die Funktion aufweisen, die Daten eines Nutzers sowohl zu löschen als auch auf sichere Weise auf andere Systeme oder Produkte zu übertragen (Anhang I Teil I Abs. 2 lit. m CRA).

b) Konkretisierung der Anforderungen mittels harmonisierter Normen

Nach Art. 27 CRA wird bei Produkten mit digitalen Elementen, die mit im EU-Amtsblatt veröffentlichten harmonisierten Normen oder Teilen davon übereinstimmen, die Konformität mit den grundlegenden Cybersicherheitsanforderungen in Anhang I des CRA (widerleglich) vermutet (sog. Konformitätsvermutung). Harmonisierte Normen spielen danach als technische Konkretisierungen der gesetzlichen Anforderungen eine wichtige Rolle bei der Erfüllung des CRA. Der notwendige Normungsauftrag (engl. Standardisation Request), welcher die Basis einer harmonisierten Norm für den CRA bilden wird, ist aktuell noch in der Verhandlung zwischen der EU-Kommission und den drei europäischen Standardisierungsorganisationen CEN, CENELEC und ETSI.[33] Aller Wahrscheinlichkeit nach wird die Normenreihe EN IEC 62443 als Grundlage für harmonisierte Normen des CRA fungieren. Die gesamte Normenreihe

28 *Wiebe*, InTeR 2021, 66, 68; *Siglmüller*, ZfPC 2023, 221, 222.
29 Vgl. https://cve.mitre.org/.
30 Eine Möglichkeit, den Schweregrad einer Schwachstelle zu bestimmen, bietet das sog. Common Vulnerability Scoring System.
31 Vgl. für Unterschiede zu der Aktualisierungspflicht in der Digitale-Inhalte-Richtlinie *Rennert*, ZfDR 2023, 206, 214.
32 Vgl. EN 18031-1:2024, 6.3.
33 Vermutlich wird ETSI diesbezüglich nur eine untergeordnete Rolle in der Normung spielen. Maßgeblich verantwortlich wird das gemeinsame technische Komitee CEN/CLC/JTC 13 und dessen WG 9 sein, welche die spezielle Arbeitsgruppe zum Cyber Resilience Act bildet.

IEC 62443 setzt sich aus bald 20 bereits veröffentlichten oder geplanten Teilen zusammen. Als harmonisierte Normen werden hiervon nur einige wenige Teile dienen, beispielsweise EN IEC 62443-4-2 und EN IEC 62443-3-3. Die Herausforderung der Normung wird darin bestehen, die Evaluierungsmethoden und Akzeptanzparameter für die Anforderungskriterien an eine Listung der Normen im EU-Amtsblatt aufzustellen. Für diese Listung muss jede harmonisierte Norm das sog. HAS-Assessment erfolgreich durchlaufen.[34] Neben diesen Herausforderungen müssen die in Betracht kommenden Normen auch hinsichtlich ihrer Sprache, der verwendeten Begriffe und Referenzen zu anderen Normen angepasst werden.

Der Anwendungsbereich der Delegierten VO (EU) 2022/30 i. V. m. der RL 2014/53/EU (sog. EU-Funkanlagenrichtlinie) überschneidet sich teilweise mit dem des CRA. Auf Basis der RL 2014/53/EU hat die Kommission einen Normungsauftrag erteilt,[35] um spezifische Normen zu entwickeln, die festlegen, wie die Cybersicherheitsanforderungen gemäß Art. 3 Abs. 3 lit. d, e und f RL 2014/53/EU umzusetzen sind. Da die Cybersicherheitsanforderungen des CRA mit den Zielen der beauftragten Normen übereinstimmen, können die im Rahmen der VO (EU) 2022/30 getätigten Normungsarbeiten im Falle einer Änderung oder Aufhebung dieser Verordnung für die Erstellung von Normen auf Grundlage des CRA wiederverwendet werden.[36]

c) Instruktive Anforderungen

Anleitungen und Informationen, die einen cybersicheren Gebrauch ermöglichen, müssen das Produkt in Papierform oder in digitaler Form begleiten (Art. 13 Abs. 18 CRA). Welche Inhalte die Anleitungen aufweisen müssen, folgt aus Anhang II des CRA, wobei Nr. 8 den Kern der cybersicherheitsrelevanten Informationen ausmacht. Dazu zählen z. B. Informationen über eine sichere Inbetriebnahme, über die Installation von Aktualisierungen und darüber, wie im Falle einer Außerbetriebnahme Nutzerdaten sicher entfernt werden können. Instruktionen sollen das Verständnis der Nutzer für die komplexe Cybersicherheitsmaterie steigern; zugleich werden sie dadurch in die Verantwortung genommen.

V. Pflichten der Wirtschaftsakteure

Der CRA erlegt den Wirtschaftsakteuren Pflichten auf, die mit den objektiven Produktanforderungen als Verkehrsfähigkeitsvoraussetzungen korrespondieren. Das Pflichtenprogramm und der -umfang hängen von der jeweiligen Rolle ab.

1. Herstellerpflichten

a) Primärverantwortung

Die Verantwortung für die Erfüllung der Produktanforderungen liegt primär bei den Herstellern. Dies zeigt allein schon der umfassende Pflichtenkanon (vgl. Artt. 13, 14 CRA). Die oberste Pflicht der Hersteller besteht in der Gewährleistung der Konformität mit den grundlegenden Cybersicherheitsanforderungen gem. Anhang I Teil I im Rahmen der Produktkonzipierung, -entwicklung und -herstellung. In diesem Zusammenhang erstrecken sich die Sorgfaltspflichten der Hersteller auch auf zugekaufte Komponenten (z. B. technische Prüfungen der Komponenten, Lieferantenauswahlprozesse). Folgerichtig hat der Hersteller außerdem geeignete Verfahren zu implementieren, die gewährleisten, dass die Produktanforderungen während der Serienherstellung durchgängig erfüllt werden (vgl. Art. 13 Abs. 14 CRA).

Der Terminus „Hersteller“ bezeichnet „eine natürliche oder juristische Person, die Produkte mit digitalen Elementen entwickelt oder herstellt oder die Produkte mit digitalen Elementen konzipieren, entwickeln oder herstellen lässt und sie unter ihrem Namen oder ihrer Marke vermarktet, sei es gegen Bezahlung, zur Monetarisierung oder unentgeltlich“ (Art. 3 Nr. 13 CRA). Daneben können nicht nur Einführer und Händler (Art. 21 CRA), sondern jede natürliche oder juristische Person (z. B. IT-Dienstleister) durch die Vornahme einer wesentlichen Änderung i. S. v. Art. 3 Nr. 30 CRA und die anschließende Bereitstellung des Produkts zum Hersteller werden (Art. 22 CRA).[37]

b) Bewertung der Cybersicherheitsrisiken

Grundlage für die Konformität mit CRA bildet die vom Hersteller durchzuführende Bewertung der Cybersicherheitsrisiken unter Beachtung der Zweckbestimmung und der vernünftigerweise vorhersehbaren Verwendung des Produkts i. S. v. Art. 3 Nrn. 23 f. CRA (Art. 13 Abs. 2 CRA). Das Ergebnis der Bewertung fließt in die Planungs-, Konzeptions-, Entwicklungs-, Herstellungs-, Liefer- und Wartungsphase des Produkts ein. Konkret dient diese Bewertung der Bestimmung, ob und welche der Cybersicherheitsanforderungen gem. Anhang I Teil I Abs. 2 des CRA auf das konkrete Produkt Anwendung finden und wie die anwendbaren Anforderungen umgesetzt werden. Die sich daran anschließende Ermittlung der anzuwendenden Cybersicherheitsmaßnahmen kann sich unter Umständen als komplex darstellen: Was bei einer bestimmten Nutzung eines Produkts in definierten Umgebungsbedingungen adäquat ist, kann bei abweichender Verwendung unzureichend sein. Eine grobe Orientierung bietet die „Je-Desto-Formel“: Je größer die Eintrittswahrscheinlichkeit eines Schadens und die potenzielle Schadenshöhe, desto mehr Cybersicherheitsmaßnahmen müssen ergriffen werden.

Bei der Bewertung der Cybersicherheitsrisiken geht es um die Untersuchung potenzieller cyberbezogener Bedrohungsszenarien und ihrer möglichen Auswirkungen auf Schutzgüter und -ziele des CRA (dazu unter III.). Zu diesem Zweck sind in Betracht kommende Cyberbedrohungen zu modellieren und die daraus entstehenden Cybersicherheitsrisiken zu beurteilen. Zur strukturierten Analyse und Bewertung der Cybersicherheitsrisiken können verschiedene Verfahren herangezogen werden. Der Ansatz der EN IEC 62443 bietet ein zyklisches Modell, das auf dem bewährten PDCA-Prinzip („Plan-Do-Check-Act“) basiert und eine wiederkehrende Durchführung von Risikoanalysen vorsieht, um auf veränderte Bedrohungslagen oder Betriebsbedingungen angemessen reagieren zu können und um den gesamten Produktlebenszyklus abzudecken.[38] Das PDCA-Prinzip umfasst vier Hauptphasen, welche zyklisch und zu jeder Phase des Lebenszyklus erneut durchlaufen werden:

34 Vgl. Assessment report under service contract SI2.876921, https://boss.cen.eu/media/BOSS%20CEN/ref/has_assessment_rep.pdf, bspw. „4.5 It does not contain non-specific or non-verifiable requirements, provisions or piece of guidance, leaving it to a manufacturer or another standard user to decide how to apply“.

35 Durchführungsbeschluss C(2022) 5637 der Kommission vom 5. 8. 2022 über einen Normungsauftrag an das Europäische Komitee für Normung und das Europäische Komitee für elektrotechnische Normung hinsichtlich Funkanlagen zur Unterstützung der RL 2014/53/EU des Europäischen Parlaments und des Rates sowie der Delegierten VO (EU) 2022/30 der Kommission.

36 Erwägungsgrund 30.

37 Vgl. *Hess*, CB 2023, 27, 30; *Dittrich/Heinelt*, RDi 2023, 309, 312.

38 Vgl. z. B. VDI/VDE 2182.

1. Plan: Planung/Bewertung der Risiken und der möglichen Gegenmaßnahmen
2. Do: Festlegung der Cybersicherheitsmaßnahmen
3. Check: Bewertung ihrer Effizienz
4. Act: Umsetzung der Cybersicherheitsmaßnahmen

Entsprechend wird der PDCA-Zyklus erstmals während der Planungsphase und im Anschluss daran während der Konzeptions- und Entwicklungsphase durchlaufen. Die grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I des CRA beeinflussen maßgeblich die Planungsphase. Ausgangspunkt ist die Identifikation der relevanten Schutzgüter, die durch die Strukturanalyse ermittelt werden. Für jedes Schutzgut werden Bedrohungen analysiert, Schutzziele definiert und die potenziellen Risiken i. d. R. qualitativ, bei vorliegenden statistischen Daten ggf. auch quantitativ bewertet. Die Risikobewertung orientiert sich dabei an Faktoren wie der Wahrscheinlichkeit eines Eintritts und der potenziellen Schadenshöhe (s. o. „Je-Desto-Formel"). Anschließend folgen die restlichen drei PDCA-Phasen und der Zyklus beginnt in der nächsten Phase des Produktlebenszyklus von vorn. Die iterative Natur des PDCA-Zyklus ermöglicht die kontinuierliche Evaluation sowie Anpassung von Cybersicherheitsmaßnahmen an die aktuelle Bedrohungslage und so die Einhaltung eines fortlaufend hohen Schutzniveaus während des gesamten Produktlebenszyklus.

Die Anzahl der möglichen Vorgehensweisen bei der Bewertung der Cybersicherheitsrisiken ist vielfältig.[39] Eine etablierte Verfahrensweise zur Identifizierung von Bedrohungen stellt die sog. STRIDE-Methode[40] dar:

- Spoofing (Identitätsverschleierung)
- Tampering (Manipulation)
- Repudiation (Verleugnung)
- Information disclosure (Verletzung der Privatsphäre oder Datenpanne)
- Denial of service (Verweigerung des Dienstes)
- Elevation of privilege (Rechteausweitung)

Die identifizierten Bedrohungen könnten mithilfe der DREAD-Methode priorisiert werden als Alternative zur matrixbasierten Feststellung der Eintrittswahrscheinlichkeit und des Schadensausmaßes. Nach der Bewertung (z. B. 1 bis 10) der einzelnen Fragen des DREAD-Merkspruchs erfolgt die Summenbildung und liefert damit eine Prioritätskennzahl für jede Bedrohung.

- Damage (Schaden) – wie schlimm wäre ein Angriff?
- Reproducibility (Reproduzierbarkeit) – wie einfach ist der Angriff zu reproduzieren?
- Exploitability (Ausnutzbarkeit) – wie viel Aufwand ist nötig, um den Angriff zu starten?
- Affected users (betroffene Benutzer) – wie viele Personen sind betroffen?
- Discoverability (Entdeckbarkeit) – wie leicht ist die Bedrohung zu entdecken?

In Abhängigkeit von der Prioritätskennzahl können im Anschluss Cybersicherheitsmaßnahmen in Übereinstimmung mit Anhang I Teil I des CRA definiert und ergriffen werden, um den identifizierten Risiken adäquat zu begegnen.[41]

c) Konformitätsbewertungsverfahren

Nach Art. 13 Abs. 12 CRA hat der Hersteller ein Konformitätsbewertungsverfahren[42] durchzuführen, das der Einhaltung der grundlegenden Cybersicherheitsanforderungen gem. Anhang I des CRA dient. Das Konformitätsbewertungsverfahren besteht entweder aus einem rein internen Kontrollverfahren oder aus Verfahren, welche die Einbindung einer (externen) notifizierten Stelle voraussetzen (vgl. Art. 32 Abs. 1 CRA).

Für Produkte mit digitalen Elementen, die nicht als kritisch oder wichtig eingestuft werden, kann der Hersteller die Konformitätsbewertung in Eigenverantwortung durchführen (internes Kontrollverfahren auf Grundlage von Modul A), vgl. Art. 32 Abs. 1 CRA. Bei wichtigen Produkten der Klasse I kann der Hersteller wählen, ob er die Konformitätsbewertung in Eigenverantwortung (Modul A) durchläuft oder die Beteiligung einer notifizierten Stelle (Module B und C oder Modul H) bevorzugt (Artt. 7, 32 Abs. 2 CRA). Bei Modul A ist die Verwendung von harmonisierten Normen, gemeinsamen Spezifikationen oder europäischen Schemata für die Cybersicherheitszertifizierung vorgeschrieben. Bei Nichtanwendung dieser Vorgaben ist die Beteiligung einer notifizierten Stelle erforderlich. Bei wichtigen Produkten der Klasse II erfordert das Konformitätsbewertungsverfahren immer die Beteiligung einer notifizierten Stelle (Module B und C oder Modul H). Dies gilt auch, wenn das Produkt vollständig oder teilweise harmonisierten Normen, gemeinsamen Spezifikationen oder europäischen Schemata für die Cybersicherheitszertifizierung entspricht (Artt. 7, 32 Abs. 3 CRA). Bei kritischen Produkten mit digitalen Elementen i. S. v. Art. 8 CRA (z. B. Smart-Meter-Gateways, vgl. Anhang IV) erfolgt der Nachweis der Konformität entweder über ein europäisches Cybersicherheitszertifikat gem. Art. 8 Abs. 1 CRA oder alternativ über eines der Verfahren, die für wichtige Produkte der Klasse II vorgesehen sind (Module B und C oder Modul H), vgl. Art. 32 Abs. 4 CRA.

Wenn ein Produkt wesentlich verändert wird, muss das Konformitätsbewertungsverfahren erneut vollzogen werden. Eine wesentliche Änderung ist jede „Änderung des Produkts mit digitalen Elementen nach dessen Inverkehrbringen, die sich auf die Konformität des Produkts mit den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I auswirkt oder zu einer Änderung des bestimmungsgemäßen Zwecks, für den das Produkt geprüft wurde, führt" (Art. 3 Nr. 30 CRA). Eine wesentliche Änderung dürfte dann anzunehmen sein, wenn die Veränderung eine neue Gefährdung aktiviert oder die Art der dem Produkt innewohnenden Gefahr ändert. Wesentlich ist sie jedenfalls auch dann, wenn ein Produkt nach der Änderung in eine höhere Risikoklasse eingeordnet werden muss.[43]

Ungelöste Probleme begegnen dem Hersteller bei der faktischen Konformitätsbewertung, z. B. bei der Evaluierung eines Produkts in einem Prüflabor. Insbesondere sind die Reproduzierbarkeit und Vergleichbarkeit von Evaluierungsergebnissen nicht ohne Weiteres gegeben. Evaluierungsergebnisse erweisen sich als subjektiv geprägt, weil sie vom Wissen und von der Erfahrung der prüfenden Person und deren Sicht auf die Bedrohungslandschaft sowie von den vom Hersteller zur Verfügung gestellten Informationen abhängen. Mehr noch: Die

39 Vgl. für eine gelungene Zusammenstellung von Methoden, um Risiken zu bewerten und Bedrohungen zu modellieren ETSI TR 103 935 V1.1.1 (2023-12), https://www.etsi.org/deliver/etsi_tr/103900_103999/103935/01.01.01_60/tr_103935v010101p.pdf.

40 Siehe auch EN 18031-1:2024, Annex A.

41 Mögliche Informationssicherheitsmaßnahmen im Bereich der Organisation können der technischen Norm EN ISO/IEC 27002:2022 entnommen werden. Auf der Produkt- bzw. Komponentenebene sind EN IEC 62443-3-3:2019 und EN IEC 62443-4-2:2019 nützliche Quellen. Praktische Beispiele für Maßnahmen im IoT-Bereich finden sich in dem technischen Bericht ETSI TR 103 621 V1.2.1 (2022-09).

42 Zu dem Konformitätsbewertungsverfahren und den einzelnen Modulen vgl. Blue Guide (Fn. 27), Abschnitt 5.

43 *Wiebe/Daelen*, 2023, 257, 261; zu den Kriterien siehe Blue Guide (Fn. 27), Abschnitt 2.1; *Schucht*, StoffR 2015, 191, 193 ff.

aktuellen technischen Normen erlauben nur eine unzureichende objektive Bewertung. So verwenden Prüfmethoden für die Cybersicherheitsbewertung häufig Negativtests, die das Fehlen von bestimmten Schwachstellen aufzeigen sollen. Da diese Prüfmittel (wie z. B. sog. Vulnerability Scanner) jedoch kontinuierlich aktualisiert werden, können mit aktualisierten Informationen neue Schwachstellen gefunden werden.[44] In anderen Prüfungssituationen kann die Dauer oder die Häufigkeit eine entscheidende Rolle spielen und bei längerer Testausführung neue Schwachstellen zu Tage bringen. Dies führt zu nicht reproduzierbaren Testergebnissen. Eine Standardisierung von Prüfaufbauten und Messumgebungen findet – anders als in anderen harmonisierten Bereichen – in cybersicherheitsbezogenen Normen nicht statt; eines der jüngsten Normungsergebnisse im Bereich der Cybersicherheit von elektronischen Produkten gesteht diese Schwäche ein.[45] Beispielsweise existieren im Bereich der elektromagnetischen Verträglichkeit (EMV) Grenzwerte für die gestrahlte oder leitungsgeführte Störaussendung,[46] Messmittelanforderungen und die Vorgaben für Prüfaufbauten.[47] Produktsicherheitsprüfungen im Zuge der Evaluierung der Sicherheitsziele der RL 2014/35/EU (sog. EU-Niederspannungsrichtlinie) werden gleichermaßen mit definierten Mess- und Prüfmitteln durchgeführt.[48]

d) Organisationspflichten

Neben produktbezogenen Pflichten treffen die Hersteller eine Reihe von Organisationspflichten. Von zentraler Bedeutung sind die Dokumentationspflichten. In concreto obliegt es den Herstellern, eine technische Dokumentation zu erstellen (Art. 13 Abs. 4 CRA). Diese enthält gem. Art. 31 Abs. 1 CRA alle einschlägigen Daten und Einzelheiten über die Einhaltung der grundlegenden Cybersicherheitsanforderungen nebst der Bewertung der Cybersicherheitsrisiken. Die technische Dokumentation ist gem. Art. 31 Abs. 2 CRA laufend zu aktualisieren und (zusammen mit der EU-Konformitätserklärung) für einen Zeitraum von mindestens 10 Jahren oder für die Dauer des Unterstützungszeitraums i. S. v. Art. 3 Nr. 20 CRA aufzubewahren (Art. 13 Abs. 13 CRA).

e) Nachmarktpflichten, insbesondere Behandlung von Schwachstellen

In Bezug auf die in Verkehr gebrachten Produkte haben die Hersteller umfangreiche produktbezogene und organisatorische Nachmarktpflichten. In diesem Zusammenhang ist die zentrale Vorschrift Art. 13 Abs. 7 CRA, wonach der Hersteller systematisch alle relevanten Cybersicherheitsaspekte zu dokumentieren hat. Dies betrifft insbesondere alle Schwachstellen, von denen der Hersteller Kenntnis erlangt. Dabei stellt Anhang I Teil II des CRA eine Reihe besonderer Pflichten in Bezug auf die Behandlung von Schwachstellen auf. Zuvorderst muss der Hersteller die Schwachstellen und Komponenten seines Produkts ermitteln und dokumentieren. Hierfür hat der Hersteller die Cybersicherheit seines Produkts im Sinne einer Produktbeobachtung regelmäßig zu testen und zu überprüfen (Anhang I Teil II Abs. 3).[49] Bei komplexer Software bzw. solcher Software, die sensible Informationen verarbeitet, kann die Durchführung externer Audits angezeigt sein (z. B. Pentests, Code-Audits). Zur Erleichterung der Schwachstellenanalyse obliegt es dem Hersteller, vorab eine Software-Stückliste i. S. v. Art. 3 Nr. 39 CRA in einem maschinenlesbaren Format zu erstellen, die alle Softwarekomponenten des Produkts auflistet.[50] Neben diese *Schwachstellenermittlungs- bzw. dokumentationspflichten* treten die anschließenden *Schwachstellenbehebungspflichten*:[51] Entdeckt der Hersteller Schwachstellen, so hat er diese während der Produktlebensdauer und des Unterstützungszeitraums i. S. v. Art. 3 Nr. 20 CRA (mindestens 5 Jahre nach dem Inverkehrbringen) wirksam zu beheben. In der Regel dürfte eine unverzügliche und kostenlose Sicherheitsaktualisierung der zu nehmende Lösungsweg sein, um Schwachstellen zu beheben.

Eine effektive Schwachstellenbehebung setzt das Vorhandensein von Mechanismen für die sichere Verbreitung von Aktualisierungen voraus. Zudem müssen entsprechende Informationen über die Schwachstelle und die Sicherheitsaktualisierungen veröffentlicht werden; vorab gilt es, eine Strategie für die koordinierte Offenlegung von Schwachstellen aufzustellen und umzusetzen (sog. *Coordinated Vulnerability Disclosure*). Abgesehen von der Schwachstellenbehebung trifft die Hersteller während des Unterstützungszeitraums die Pflicht, auch bei sonstigen Nichtkonformitäten erforderliche Korrekturmaßnahmen zu ergreifen (Art. 13 Abs. 21 CRA).

Nach Art. 13 Abs. 22 CRA müssen Hersteller mit den Marktüberwachungsbehörden kooperieren. Auf deren begründetes Verlangen hin haben sie insbesondere alle Informationen und Unterlagen, die für den Konformitätsnachweis erforderlich sind, zur Verfügung zu stellen. Die Marktüberwachungsbehörde kann den Hersteller zur Zusammenarbeit bei Maßnahmen zur Abwendung von Cybersicherheitsrisiken auffordern. In diesem Kontext spielen die in Art. 14 CRA aufgestellten Meldepflichten gegenüber der Agentur der Europäischen Union für Cybersicherheit (ENISA) eine wichtige Rolle.[52] Der Hersteller hat gem. Art. 14 Abs. 2 lit. a CRA unverzüglich (spätestens nach 24 Stunden) eine Frühwarnung über eine aktiv ausgenutzte Schwachstelle i. S. v. Art. 3 Nr. 42 CRA über die Meldeplattform nach Art. 16 CRA abzusetzen. Spätestens nach 72 Stunden sind Informationen über das betreffende Produkt mit digitalen Elementen, über die allgemeine Art der Ausnutzung und der betreffenden Schwachstelle sowie über alle ergriffenen Korrektur- oder Risikominderungsmaßnahmen sowie Abhilfemaßnahmen, die Nutzer ergreifen können, zu übermitteln. Spätestens nach 14 Tagen ist ein Abschlussbericht vorzulegen. Eine vom Prinzip her ähnlich zeitlich abgestufte Meldepflicht besteht auch bei einem schwerwiegenden Sicherheitsvorfall nach Art. 14 Abs. 3 CRA. Meldepflichten existieren ebenso gegenüber der Lieferkette (Art. 13 Abs. 6 CRA): Rührt die Schwachstelle von einer in das Produkt integrierten (inklusive quelloffenen) Komponente her, ist diejenige Person oder Einrichtung über diese Schwachstelle zu informieren, die diese Komponente herstellt oder wartet (im Regelfall der Entwickler).[53] Im Übrigen ist der Hersteller verpflichtet, vor der Einstellung seines Betriebs die Marktüberwachungsbehörden darüber zu unterrichten. Soweit es dem Hersteller mit den ihm zur Verfügung stehenden Mitteln möglich ist, muss er ebenso die Nutzer der betroffenen Produkte über die Betriebseinstellung informieren (vgl. Art. 13 Abs. 23 CRA).

44 Vgl. https://www.iecee.org/certification/iec-standards/etsi-303-64520 20.
45 EN 18031-1:2024, A.2.8.3 Security testing.
46 Siehe EN 55011:2016 + A1:2017 + A11:2020 + A2:2021, Tabelle 2 bis 17.
47 Siehe EN 55011:2016 + A1:2017 + A11:2020 + A2:2021, Abschnitt 7.3 bis 7.5.
48 Siehe EN 60335-1:2012 + A11:2014 + A13:2017 + A1:2019 + A2:2019 + A14:2019, Abschnitt 22.11 und Bild 7.
49 Vgl. für die digitale Produktbeobachtung *Schucht/Piovano/Wiebe*, Quick Guide: Produktbeobachtung in der Digitalisierung, 2023, S. 77 ff.
50 Erwägungsgrund 77.
51 *Wiebe/Daelen*, EuZW 2023, 257, 261.
52 Vgl. zu den Meldepflichten des CRA *Erdelt*, ZfPC 2024, 176.
53 *Dittrich/Heinelt*, RDi 2023, 309, 313.

2. Einführerpflichten

Nach Art. 19 Abs. 1 CRA darf der Einführer nur Produkte in den Verkehr bringen, die den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I des CRA genügen und bei denen die vom Hersteller festgelegten Verfahren den Vorgaben aus Anhang I Teil II des CRA entsprechen. Gleichwohl treffen den Einführer gem. Art. 19 Abs. 2 CRA nur formelle Sicherstellungspflichten, vor allem in Bezug auf ein durchgeführtes Konformitätsbewertungsverfahren, die technische Dokumentation, die EU-Konformitätserklärung sowie die Erfüllung der Informations- und Kennzeichnungsvorgaben. Stellt der Einführer im Rahmen dieser Prüfung Nichtkonformitäten fest oder hat einen entsprechenden Verdacht, so muss er diese (regelmäßig zusammen mit dem Hersteller) vor dem Inverkehrbringen beheben und im Falle eines erheblichen Cybersicherheitsrisikos die Marktüberwachungsbehörden unterrichten (Art. 19 Abs. 3 CRA).

Auch mit Blick auf bereits in Verkehr gebrachte nonkonforme Produkte sorgt er für die Ergreifung erforderlicher Korrekturmaßnahmen (vgl. Art. 19 Abs. 5 UAbs. 1 CRA). Entdeckt der Einführer eine Schwachstelle, ist er gehalten, den Hersteller umgehend darüber zu informieren (Art. 19 Abs. 5 UAbs. 2 S. 1 CRA). Sollte diese Schwachstelle ein erhebliches Cybersicherheitsrisiko darstellen, liegt es zusätzlich in der Verantwortung des Einführers, die Marktüberwachungsbehörden über die festgestellte Nichtkonformität und die ergriffenen Maßnahmen in Kenntnis zu setzen (Art. 19 Abs. 5 UAbs. 2 S. 2 CRA). Darüber hinaus sind Einführer – ebenso wie Hersteller – verpflichtet, mit den zuständigen Marktüberwachungsbehörden eng zusammenzuarbeiten (Art. 19 Abs. 7 CRA).

3. Händlerpflichten

Im Vormarktbereich sehen sich Händler nur formellen Prüfpflichten konfrontiert. Sie müssen nach Art. 20 Abs. 2 CRA im Wesentlichen die Einhaltung der Informations- und Kennzeichnungsanforderungen (stichprobenartig) überprüfen. Bei fehlender Konformität besteht auch für Händler ein gesetzliches Verkehrsverbot (Art. 20 Abs. 3 CRA). Im Nachmarktbereich haben Händler (nachrangige) Gefahrabwendungs- und Notifikationspflichten (Art. 20 Abs. 4 CRA). In Art. 20 Abs. 5 CRA sind schließlich noch Kooperationspflichten gegenüber den Marktüberwachungsbehörden geregelt.

VI. Durchsetzung des CRA

Die behördliche Marktüberwachung und Durchsetzung des CRA erfolgt auf Basis der VO (EU) 2019/1020 (sog. EU-Marktüberwachungsverordnung), vgl. Art. 52 Abs. 1 CRA. Die Marktüberwachungsbehörden können die Wirtschaftsakteure zur Ergreifung von Korrekturmaßnahmen auffordern oder entsprechende Maßnahmen anordnen bzw. selbst ergreifen, wenn ein in Verkehr gebrachtes Produkt die Anforderungen des CRA nicht erfüllt. Birgt ein Produkt ein erhebliches Cybersicherheitsrisiko, haben die Marktüberwachungsbehörden die Möglichkeit, einen Rückruf oder bei Softwareprodukten eine Stilllegung anzuordnen.

Art. 64 CRA sieht erhebliche Sanktionsmöglichkeiten vor, die die Mitgliedstaaten im nationalen Recht verankern müssen. Bei Nichteinhaltung der grundlegenden Cybersicherheitsanforderungen oder einem Verstoß gegen die Herstellerpflichten gem. den Artt. 13, 14 CRA kommen Geldbußen von bis zu EUR 15 Millionen oder von bis zu 2,5 % des gesamten weltweiten Jahresumsatzes in Betracht – je nachdem, welcher Betrag höher ist (Art. 64 Abs. 2 CRA). Mit Blick auf die übrigen Wirtschaftsakteure sollen Geldbußen von bis zu EUR 10 Millionen oder von bis zu 2,0 % des Umsatzes möglich sein (Art. 64 Abs. 3 CRA).[54]

VII. Fazit und Blick nach vorne

Der CRA markiert einen bedeutenden Schritt bei der Regulierung der produktbezogenen Cybersicherheit. Mit den umfassenden Anforderungen an Cybersicherheit und den korrespondierenden Pflichten der Wirtschaftsakteure versucht der CRA, ein hohes Niveau beim Schutz vor produktbezogenen Cyberbedrohungen zu setzen. Dies fördert nicht nur das Vertrauen der Nutzer in innovative Produkte mit digitalen Elementen, sondern stärkt auch den fairen Wettbewerb.[55] Als Kehrseite bringt der CRA aus unternehmerischer Sicht (insbesondere für kleine und mittlere Unternehmen) ohne Zweifel nicht zu unterschätzende Herausforderungen mit sich; dies gilt vor allem vor dem Hintergrund der Normungsprobleme und der Schwierigkeiten bei der Konformitätsbewertung. Ob der CRA Innovationen hemmen oder sogar zur Steigerung der Wettbewerbsfähigkeit europäischer Unternehmen beitragen wird, bleibt abzuwarten.

Freilich dürften viele Hersteller schon jetzt aus Eigeninteresse und aus haftungsrechtlichen Erwägungen[56] produktbezogene Cybersicherheitsvorkehrungen und Maßnahmen zur Cyberwiderstandsfähigkeit ergreifen. Jedenfalls ist den betroffenen Wirtschaftsakteuren anzuraten, sich zeitnah mit dem CRA auseinanderzusetzen. Denn sie haben (nur) bis zum 11. 12. 2027 Zeit, die Vorgaben des CRA umzusetzen (Art. 71 Abs. 1 CRA). Die Meldepflichten für aktiv ausgenutzte Sicherheitslücken gem. Art. 14 CRA gelten bereits ab dem 11. 9. 2026, die Vorschriften über die Notifizierung von Konformitätsbewertungsstellen (Kapitel IV des CRA) ab dem 11. 6. 2026.

Dr. Gerhard Wiebe

ist Rechtsanwalt in der Produktkanzlei und berät internationale und nationale Unternehmen zu Product-Compliance-Themen (insb. Produktsicherheits- und Produkthaftungsrecht). Dabei nimmt er insbesondere auch die stetig wachsenden cybersicherheitsrechtlichen Produktanforderungen in den Blick.

Johannes Daelen

LL.M., ist wissenschaftlicher Mitarbeiter in der Produktkanzlei und bearbeitet schwerpunktmäßig produktrechtliche Fragestellungen mit Bezug zu digitalen Produkten. Dabei behält er insbesondere die einschlägige EU-Gesetzgebung zu den in Zukunft dominierenden Themen wie Cybersicherheit und Künstlicher Intelligenz (KI) im Blick.

Benjamin Kerger

B. Eng.; ist bei GLOBALNORM als Product Compliance Consultant tätig. Zuvor war er Laborleiter für Produktsicherheit. Nach dem Studium der Nachrichtentechnik begann er seinen Dienst 2013 bei einem Prüf- und Zertifizierungsdienstleister im Bereich Funk und EMV.

54 Vgl. *Rennert*, ZfDR 2023, 206, 214; *Dittrich/Heinelt*, 2023, 309, 316.

55 Ein weniger positives Fazit zum CRA-Entwurf zieht *Siglmüller*, ZfPC 2023, 221, 223; vgl. auch *Dittrich/Heinelt*, RDi 2023, 309, 316.

56 *Wiebe*, InTeR 2021, 66, 67 ff.