Vorschlag COM(2022) 454 vom 15. September 2022 für eine **Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen** und zur Änderung der Verordnung (EU) 2019/1020.

CYBERRESILIENZGESETZ (CYBER RESILIENCE ACT)

cep**Analyse** Nr. 1/2023

LANGFASSUNG

Autorin: Dr. Anastasia Kotovskaia, LL.M. | kotovskaia@cep.eu

A. Wesentliche Inhalte des EU-Vorhabens

1 Hintergrund und Ziele

- Laut Kommission sind Soft- und Hardwareprodukte in den letzten Jahren immer häufiger von Cyberattacken betroffen gewesen. Ein wesentlicher Grund hierfür ist ein geringes Maß an Cybersicherheit dieser Produkte, die oft Schwachstellen aufweisen, die nur unzureichend oder verspätet geschlossen werden. [Begründung S. 1]
- Allein 2021 entstanden weltweit Schäden durch Cyberkriminalität in Höhe von 5,5 Billionen Euro. Als erfolgreiche Cyberangriffe, die aus einer mangelnden Cybersicherheit von Soft- und Hardwareprodukten resultieren, gelten u.a. der Ramsonware-Wurm „WannaCry“, welcher eine Schwachstelle in „Windows“ ausnutzte und der Kaseya VSA-Angriff, bei dem eine Netzverwaltungssoftware von Kaseya Sicherheitslücken aufwies. [Begründung S. 1]
- Cybersicherheitsvorfälle bei Produkten mit digitalen Elementen können Auswirkungen auf Organisationen und Lieferketten haben, sich rasch im ganzen Binnenmarkt verbreiten und zu „erheblichen gesellschaftlichen und wirtschaftlichen Kosten“ führen. Jedoch gibt es für die meisten Hard- und Softwareprodukte bisher keine EU-Rechtsvorschriften, die auf deren Cybersicherheit abzielen. [Begründung S. 1]
- Die Kommission hat daher einen Vorschlag für ein Cyberresilienzgesetz (Cyber Resilience Act, CRA) vorgelegt. Mit dem CRA wird ein Rechtsrahmen für die Entwicklung und das Inverkehrbringen von cybersicheren Produkten mit digitalen Elementen (im Folgenden kurz „PmdE“) in der EU geschaffen. [Begründung S. 1]
- Der CRA etabliert insbesondere [Art. 1]
  - Anforderungen an die Konzeption, Entwicklung, Herstellung und das Inverkehrbringen von PmdE,
  - Pflichten für relevante Wirtschaftsakteure, d.h. Hersteller, Einführer und Händler,
  - Anforderungen zum Umgang mit Schwachstellen, sowie
  - Vorgaben zur Überwachung des Marktes für PmdE und zur Durchsetzung der Anforderungen des CRA.
- Ziel der Kommission ist es insbesondere, [Begründung S. 1 und 8, Erwägungsgründe 1, 2 und 4]
  - einheitliche Cybersicherheitsvorschriften für Hersteller, Einführer und Händler von PmdE zu etablieren,
  - sicherzustellen, dass Hersteller von PmdE die Cybersicherheit ihrer Produkte bereits in der Konzeptions- und Entwicklungsphase verbessern, sodass diese mit weniger Schwachstellen auf den Markt kommen,
  - sicherzustellen, dass sich die Hersteller auch während des Produktlebenszyklus „ernsthaft“ um etwaige Cybersicherheitsrisiken kümmern,
  - die Transparenz über die Sicherheitseigenschaften von PmdE zu stärken, damit Produktnutzer die Cybersicherheitsmerkmale eines Produkts bei der Kaufentscheidung besser einschätzen können,
  - die Anzahl von Cybersicherheitsvorfällen und damit einhergehende Kosten und Reputationsschäden für Hersteller, Einführer und Händler der PmdE zu reduzieren, und
  - die Attraktivität von PmdE aus der EU zu stärken.

2 Anwendungsbereich

- Der CRA gilt für alle „Produkte mit digitalen Elementen (PmdE)“. „PmdE“ sind „verbindungsfähige“ Softwareprodukte- bzw. Hardwareprodukte, deren Verwendung eine Datenverbindung zu einem Gerät oder Netzwerk umfasst. Auch Software- und Hardwarekomponenten, die getrennt in Verkehr gebracht werden sollen („non-embedded“), gelten als „PmdE“. Zudem umfasst „PmdE“ auch etwaige „Datenfernverarbeitungslösungen“ der Soft- und Hardwareprodukte, ohne die das PmdE eine seiner Funktionen nicht erfüllen könnte. [Erwägungsgrund 10, Art. 2 Abs. 1, Art. 3 Ziff. 1, 2 und 6–12]
- Der CRA gilt nicht für PmdE, sofern sie [Art. 2 Abs. 2]
  - Medizinprodukte oder In-vitro-Diagnostika für den menschlichen Gebrauch, und
  - Kraftfahrzeuge, sowie Systeme, Bauteile und technische Einheiten dieser Fahrzeuge, sind.

  Für diese gibt es bereits sektorspezifische Cybersicherheitsvorschriften [Erwägungsgründe 12 und 13].
- Der CRA gilt zudem nicht für PmdE, sofern diese [Erwägungsgrund 10, Art. 2 Abs. 3 und 5]
  - luftfahrttechnische Erzeugnisse, Teile und Ausrüstungen sind und nach der Verordnung zur Zivilluftfahrt (EU) 2018/1139 bereits bezüglich Sicherheitsanforderungen zertifiziert wurden,
  - ausschließlich für Zwecke der nationalen Sicherheit oder des Militärs entwickelt wurden,
  - speziell der Verarbeitung von Verschlusssachen dienen, oder

  - freie und quelloffene Softwareprodukte („Open-Source“) sind, die außerhalb einer Geschäftstätigkeit entwickelt oder bereitgestellt werden.

- Die Anwendung des CRA kann eingeschränkt oder ausgeschlossen werden, wenn andere EU-Vorschriften Regelungen enthalten, die mit den grundlegenden Anforderungen des CRA vergleichbar sind. Das gilt nur, wenn [Art. 2 Abs. 4]:
  - die Einschränkung bzw. der Ausschluss mit den bestehenden Vorschriften für diese PmdE vereinbar ist,
  - die sektorspezifischen Vorschriften das gleiche Schutzniveau wie der vorgeschlagene CRA garantieren.

  Die Kommission kann hierzu delegierte Rechtsakte erlassen.

3 Produkte mit digitalen Elementen – Einteilung in vier Gruppen

- PmdE werden grundsätzlich in vier Gruppen, abhängig von ihrem Risikograd unterteilt [Art. 6 Abs. 1 und 5, Erwägungsgründe 26, 27 und 62]:
  - Nicht-kritische PmdE: Das sind PmdE, die nicht unter eine der anderen Gruppen fallen. Dazu zählen u.a. Festplatten, Textverarbeitungssoftware und PC-Spiele.
  - Kritische PmdE (Klasse I): Dazu zählen u.a., Browser, Software zum Entfernen von Schadsoftware und Passwort-Manager.
  - Kritische PmdE (Klasse II): Dazu zählen u.a. Betriebssysteme für Server, Desktops und Handys, Public-Key-Infrastrukturen, Firewalls für den industriellen Einsatz, Router, Sicherheitselemente, Chipkarten und Chipkartenleser.
  - Hochkritische PmdE: Unter diese Gruppe fallen zu Beginn noch keine PmdE.

  In die Gruppe der nicht-kritischen PmdE soll ca. 90% des Marktes fallen. Nicht mehr als 10% des Marktes sollen als kritisch gelten [Folgenabschätzung Part 1/3, S. 48]. Für eine Übersicht mit Beispielen zur Einstufung von PmdE: siehe Anhang I.

- Die Kommission kann mittels delegierter Rechtsakte die Listen der kritischen PmdE – Klasse I und II – um neue Kategorien kritischer Produkte ergänzen bzw. einzelne Kategorien aus diesen Listen entfernen. Hierbei berücksichtigt sie den Grad des Cybersicherheitsrisikos der jeweiligen Produktkategorie und trifft ihre Entscheidung auf Basis der folgenden Kriterien [Art. 6 Abs. 2]:
  - cybersicherheitsbezogene Funktionalität des PmdE,
  - Einsatz des PmdE in sensiblen Umgebungen, z.B. in industriellen Umgebungen oder durch „wesentliche“ Einrichtungen – z.B. Energieversorger, Flughäfen, Betreiber von Internet-Knoten – im Sinne der NIS 2-Richtlinie (s. cep**Adhoc**),
  - Ausmaß von Verlusten oder Störungen, die durch den Einsatz eines PmdE bereits entstanden sind, und
  - Anlass zu erheblichen Bedenken, dass nachteilige Auswirkungen durch die Nutzung eines PmdE entstehen könnten.

- Die Kommission kann mittels delegierter Rechtsakte eine Liste mit Kategorien von hochkritischen PmdE erstellen. Dabei prüft sie insbesondere, ob eine Produktkategorie [Art. 6 Abs. 5]
  - eine oder mehrere der Kriterien zur Bestimmung der kritischen PmdE der Klasse 1 und 2 erfüllt,
  - von „wesentlichen“ Einrichtungen im Sinne der NIS 2-Richtlinie genutzt wird oder für deren Tätigkeiten potenziell von Bedeutung sein werden, oder
  - für die Widerstandsfähigkeit der Lieferkette von PmdE relevant ist.

4 Sicherheitsanforderungen an Produkte mit digitalen Elementen

- PmdE müssen u.a. [Anhang I Teil 1 Abschnitt 1]
  - so konzipiert, entwickelt und hergestellt werden, dass sie ein angemessenes Cybersicherheitsniveau gewährleisten,
  - ohne bekannte ausnutzbare Schwachstellen ausgeliefert werden,
  - in einer sicheren Standardkonfiguration bereitgestellt werden,
  - die Möglichkeit bieten, das Produkt in seine Standardkonfiguration zurückzusetzen,
  - geeignete Kontrollmechanismen gegen unbefugten Zugriff enthalten,
  - die Vertraulichkeit und Integrität personenbezogener und sonstiger Daten gewährleisten,
  - das Prinzip der „Datenminimierung“ achten; die Datenverarbeitung muss daher auf das für die intendierte Verwendung des Produkts erforderliche Maß beschränkt sein, und
  - gewährleisten, dass zur Behebung von Schwachstellen Sicherheitsaktualisierungen zur Verfügung stehen.

5 Anforderungen zum Umgang mit Schwachstellen

- Unter einer „Schwachstelle“ versteht man die „Schwäche, Anfälligkeit oder Fehlfunktion“ eines IKT-Produkts oder IKT-Dienstes, welche bei einer Cyberbedrohung ausgenutzt werden kann [Art. 3 Ziff. 39 i.V.m. Art. 6 Ziff. 15 NIS 2-Richtlinie].

- Hersteller von PmdE müssen u.a. [Anhang I Teil 1 Abschnitt 2]
  - Schwachstellen und Komponenten des Produkts identifizieren und dokumentieren, etwa in einer „Software-Stückliste“ (Software Bill Of Materials, SBOM), d.h. eine Aufzeichnung der Komponenten, die in den Softwareelementen eines PmdE enthalten sind,
  - Schwachstellen „unverzüglich“ adressieren und beheben,
  - sicherstellen, dass Sicherheitspatches und -aktualisierungen „unverzüglich“ und „kostenlos“ bereitgestellt werden, sobald sie zur Verfügung stehen,
  - die Sicherheit ihres PmdE regelmäßig testen,
  - Informationen über behobene Schwachstellen öffentlich bekannt geben, sobald sie Sicherheitsaktualisierungen bereitgestellt haben, und
  - Maßnahmen zur Erleichterung des Austauschs von Informationen über potenzielle Schwachstellen in ihrem Produkt mit Dritten ergreifen.

6 Verpflichtungen der Wirtschaftsakteure

Der CRA etabliert horizontale Anforderungen an alle Wirtschaftsakteure im Wertschöpfungsnetzwerk eines PmdE, d.h. insbesondere den Herstellern, Einführern und Händlern [Chapter II, Art. 3 Abs. 1 Ziff. 17].

6.1 Verpflichtungen der Hersteller

- Hersteller von PmdE müssen vor deren Inverkehrbringen insbesondere
  - sicherstellen, dass diese den Sicherheitsanforderungen (s. Abschnitt 4) entsprechen [Art. 10 Abs. 1],
  - die mit dem Produkt verbundenen Cybersicherheitsrisiken bewerten [Art. 10 Abs. 2],
  - erhaltene Erkenntnisse aus der Bewertung bei der Planung, Konzeption, Entwicklung, Herstellung, Lieferung und der Wartung des Produkts berücksichtigen [Art. 10 Abs. 2],
  - eine technische Dokumentation erstellen (näheres hierzu s. Abschnitt 7) [Art. 10 Abs. 7], und
  - Konformitätsbewertungsverfahren durchführen bzw. durchführen lassen (näheres hierzu s. Abschnitt 7) [Art. 10 Abs. 7].

- Hersteller von PmdE müssen ferner insbesondere
  - relevante, die Cybersicherheit ihres Produkts betreffende Aspekte systematisch dokumentieren, inklusive der Schwachstellen, von denen er Kenntnis erlangt [Art. 10 Abs. 5],
  - für eine Behebung von Schwachstellen sorgen; dies gilt, je nachdem, welcher Zeitraum kürzer ist, für [Art. 10 Abs. 6]
    - die voraussichtliche Lebensdauer des Produkts, oder
    - fünf Jahre ab dem Zeitpunkt des Inverkehrbringens des Produkts,
  - über Strategien und Verfahren verfügen, um Schwachstellen zu beheben, die ihnen gemeldet wurden, inklusive Strategien zur Offenlegung der Schwachstellen [Art. 10 Abs. 6], und
  - „unverzüglich“ – für die voraussichtliche Lebensdauer des Produkts oder fünf Jahre ab dem Zeitpunkt des Inverkehrbringens des Produkts, je nachdem, welcher Zeitraum kürzer ist, – Abhilfemaßnahmen ergreifen, sofern sie wissen oder Grund zu der Annahme haben, dass ihr PmdE nicht den Sicherheitsanforderungen (Abschnitt 4) bzw. den Anforderungen zum Umgang mit Schwachstellen (Abschnitt 5) entspricht; dies kann auch den Rückruf oder die Rücknahme des Produkts umfassen [Art. 10 Abs. 12].

- Hersteller von PmdE müssen den Produktnutzern Informationen und Anleitungen zur Verfügung stellen, u. a. [Art. 10 Abs. 10, Anhang 2]:
  - zu den Kontaktdaten des Herstellers,
  - zu der Kontaktstelle, der Informationen über Schwachstellen gemeldet werden können,
  - zur beabsichtigten Verwendung des Produktes und dessen zentrale Funktionen,
  - Informationen, unter welchen Umständen bei der Nutzung des Produkts Cybersicherheitsrisiken eintreten könnten,
  - zum technischen Support, inklusive Informationen darüber, wie lange der Nutzer mit Sicherheitsupdates rechnen kann,

  - zur sicheren Erstinbetriebnahme des Produkts, zur Installation von Sicherheitsaktualisierungen, und zur sicheren Außerbetriebnahme des Produkts.

- Hersteller von PmdE müssen ferner jeden, ihr PmdE betreffenden Cybersicherheitsvorfall sowie jede aktiv ausgenutzte Schwachstelle binnen 24 Stunden der Agentur der Europäischen Union für Cybersicherheit (ENISA) melden. Die Meldung muss Informationen zum Vorfall bzw. zur Schwachstelle enthalten. [Art. 11 Abs. 1 und 2] Meldungen zu massiven Cybersicherheitsvorfälle und -krisen auf operativer Ebene muss die ENISA dem Europäischen Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) weiterleiten [Art. 11 Abs. 3].
- Hersteller von PmdE müssen auch die Nutzer der PmdE über Cybersicherheitsvorfälle informieren und ihnen ggfs. mitteilen, welche Maßnahmen sie ergreifen können, um die Folgen eines Vorfalls zu begrenzen [Art. 11 Abs. 4]. Die Hersteller können ihre Kunden entweder direkt kontaktieren oder eine Meldung auf ihrer Webseite veröffentlichen [Erwägungsgrund 35].
- Hersteller von PmdE müssen Schwachstellen in einer Komponente, die in ihr PmdE integriert ist, an die Person oder Einrichtung melden, die die Komponente wartet [Art. 11 Abs. 7].

6.2 Verpflichtungen der Einführer und Händler

- Einführer dürfen PmdE nur dann in Verkehr bringen, wenn diese den Sicherheitsanforderungen (s. Abschnitt 4) und den Anforderungen zum Umgang mit Schwachstellen (Abschnitt 5) genügen [Art. 13 Abs. 1]. Dafür müssen sie prüfen, ob das PmdE des Herstellers ein Konformitätsbewertungsverfahren durchlaufen hat, eine technische Dokumentation vorliegt und ob das Produkt mit dem CE-Kennzeichen versehen ist [Art. 13 Abs. 2].
- Händler müssen beim Inverkehrbringen eines PmdE „mit gebührender Sorgfalt“ darauf achten, dass die Anforderungen des CRA erfüllt sind. Sie müssen u.a. prüfen, ob das Produkt mit dem CE-Kennzeichen versehen ist und die Informationen und Anleitungen des Herstellers zum Produkt zur Verfügung stehen. [Art. 14 Abs. 1 und 2]
- Stellt ein Einführer oder ein Händler fest, dass die Anforderungen nicht erfüllt sind, dürfen sie das PmdE so lange nicht Inverkehrbringen, bis die Anforderungen erfüllt sind [Art. 13 Abs. 3, Art. 14 Abs. 3]. Stellen sie fest, dass ein PmdE die Anforderungen nach dessen Inverkehrbringen nicht erfüllt, sorgen sie „unverzüglich“ dafür, dass die erforderlichen Korrekturmaßnahmen ergriffen werden oder nehmen das betroffene Produkt ggfs. vom Markt bzw. rufen es zurück [Art. 13 Abs. 6, Art. 14 Abs. 4].
- Besteht ein erhebliches Cybersicherheitsrisiko, müssen Einführer und Händler den Hersteller und die Marktüberwachungsbehörden darüber informieren [Art. 13 Abs. 3 und 6, Art. 14 Abs. 3].
- Einführer müssen sicherstellen, dass dem PmdE die Informationen und Anleitungen des Herstellers zum Produkt beigefügt sind [Art. 13 Abs. 5].
- Einführer und Händler müssen den Marktüberwachungsbehörden auf deren Ersuchen alle Informationen bereitstellen, die die Konformität des PmdE mit den Anforderungen nachweisen [Art. 13 Abs. 8, Art. 14 Abs. 5].

7 Konformitätsbewertungsverfahren

Durch eine „Konformitätsbewertung“ wird überprüft, ob ein PmdE die Sicherheitsanforderungen (Abschnitt 4) und die Anforderungen zum Umgang mit Schwachstellen (Abschnitt 5) erfüllt [Art. 31 Ziff. 21];

7.1 Vermutung der Konformität

- Bei PmdE wird eine Konformität mit den Cybersicherheitsanforderungen „vermutet“, wenn
  - diese mit harmonisierten EU-Normen oder Teilen davon übereinstimmen [Art. 18 Abs. 1].
  - diese mit „gemeinsamen Spezifikationen“ übereinstimmen, welche die Kommission mittels Durchführungsrechtsakten erlassen hat; dies gilt, wenn es für die PmdE keine oder nur unzureichende harmonisierten EU-Normen gibt [Art. 18 Abs. 2 und Art. 19], oder
  - für diese, im Rahmen eines EU-Cybersicherheitszertifizierungssystems gemäß der Verordnung (EU) 2019/881 (s. cep**Analyse**), eine EU-Konformitätserklärung oder ein Zertifikat ausgestellt wurde [Art. 18 Abs. 3].
- Die Kommission kann mittels Durchführungsrechtsakten u.a. die EU-Cybersicherheitszertifizierungssysteme festlegen, die zum Nachweis der Konformität eines PmdE genutzt werden können [Art. 18 Abs. 4].

7.2 Konformitätsbewertung

- Es werden Konformitätsbewertungsverfahren etabliert. Mit diesen soll die Einhaltung produkt- und prozessbezogener Anforderungen während des gesamten Lebenszyklus von PmdE geprüft werden. Dabei wird auf Module für solche Verfahren zurückgegriffen, die sich nach dem Risiko und dem erforderlichen Sicherheitsniveau richten. [Erwägungsgrund 44]
- Hersteller von PmdE können zur Konformitätsbewertung auf drei mögliche Verfahren zurückgreifen [Art. 24 Abs. 1 i.V.m. Annex VI und Beschluss Nr. 768/2008/EG]:
  1. internes Kontrollverfahren (Modul A),
  2. EU-Baumusterprüfverfahren (Modul B) gefolgt von dem auf der internen Fertigungskontrolle basierenden Verfahren (Modul C), oder
  3. umfassende Qualitätssicherung (Modul H).

  Für mehr Details zu den einzelnen Modulen, s. Anhang II.
- Hersteller von nichtkritischen PmdE (Gruppe 1) können die Konformität ihres Produkts durch eine „Selbstbewertung“ nach dem Verfahren auf der Grundlage von Modul A prüfen. Sie können auf freiwilliger Basis auch ein strengeres Konformitätsbewertungsverfahren wählen. [Erwägungsgrund 45]
- Hersteller von kritischen PmdE der Klasse 1 (Gruppe 2) müssen die Konformität ihres Produkts nach den Verfahren auf der Grundlage der Module B und C oder des Moduls H prüfen. Gibt es harmonisierte EU-Standards, gemeinsame Spezifikationen oder EU-Zertifizierungssysteme können sie auch auf diese zur Konformitätsbewertung zurückgreifen. [Art. 24 Abs. 2]
- Hersteller von kritischen PmdE der Klasse 2 (Gruppe 3) müssen die Konformität ihres Produkts nach den Verfahren auf der Grundlage der Module B und C oder des Moduls H prüfen [Art. 24 Abs. 3]. Die Konformitätsbewertung muss dabei immer von einer dritten Partei durchgeführt werden [Erwägungsgrund 45].
- Hersteller von hochkritischen PmdE (Gruppe 4) müssen die Konformität ihres Produkts durch Erlangen eines europäischen Cybersicherheitszertifikat im Rahmen eines EU-Zertifizierungssystems nachweisen [Art. 6 Abs. 5].
- Hersteller von PmdE müssen eine EU-Konformitätserklärung ausstellen. Diese muss laufend aktualisiert werden und die Erfüllung der Anforderungen bescheinigen [Art. 20 Abs. 1].

7.3 Technische Dokumentation und CE-Kennzeichen

- Hersteller müssen vor dem Inverkehrbringen ihres PmdE eine „technische Dokumentation“ erstellen [Art. 10 Abs. 7 i.V.m. Annex V]. Diese muss Angaben zu den Mitteln enthalten, die der Hersteller für die Erfüllung der grundlegenden Anforderungen einsetzt [Art. 23 Abs. 1]. Die technische Dokumentation muss, je nachdem, welcher Zeitraum kürzer ist, während der voraussichtlichen Produktlebensdauer oder eines Zeitraums von fünf Jahren nach dem Inverkehrbringen des Produkts laufend aktualisiert werden [Art. 23 Abs. 2].
- Hersteller müssen vor dem Inverkehrbringen ihres PmdE am Produkt das „CE-Kennzeichen“ anbringen [Art. 10 Abs. 7, Art. 22]. Mit diesem signalisiert der Hersteller, dass das Produkt die Sicherheitsanforderungen (Abschnitt 4) und die Anforderungen zum Umgang mit Schwachstellen (Abschnitt 5) erfüllt [Art. 2 Ziff. 32].

8 Marktüberwachung und Durchsetzung

8.1 Rolle und Befugnisse der Marktüberwachungsbehörden und der Kommission

- Jeder Mitgliedstaat bestimmt eine oder mehrere Marktüberwachungsbehörden [Art. 41 Abs. 2].
- Ist eine Marktüberwachungsbehörde eines Mitgliedstaats der Auffassung, dass ein PmdE ein „erhebliches Cybersicherheitsrisiko“ darstellt, kann sie eine Bewertung des Produkts vornehmen. Gelangt sie zu dem Ergebnis, dass das Produkt die Anforderungen des CRA nicht erfüllt, fordert sie den betroffenen Marktakteur „unverzüglich“ auf, geeignete Korrekturmaßnahmen zu ergreifen, das Produkt vom Markt zu nehmen oder es zurückzurufen. [Art. 43 Abs. 1]
- Betrifft das Risiko nicht nur das Hoheitsgebiet der Marktüberwachungsbehörde, muss diese die Kommission und die anderen Mitgliedstaaten über die Bewertung und die getroffenen Korrekturmaßnahmen informieren [Art. 43 Abs. 2].

- Ergreift der Hersteller eines PmdE keine angemessenen Korrekturmaßnahmeneines innerhalb der gesetzten Frist, muss die Marktüberwachungsbehörde geeignete „vorläufige“ Maßnahmen treffen. Das umfasst auch die Untersagung oder Einschränkung der Bereitstellung des Produkts auf ihrem nationalen Markt. Die Behörde muss darüber auch die Kommission und die anderen Mitgliedstaaten informieren. [Art. 43 Abs. 4]
- Gibt es binnen drei Monaten nach Einleiten einer vorläufigen Maßnahme keine Einwände gegen diese vonseiten eines Mitgliedstaates oder der Kommission, dann gilt diese Maßnahme als gerechtfertigt. Die Marktüberwachungsbehörden aller Mitgliedstaaten stellen dann sicher, dass „unverzüglich“ geeignete restriktive Maßnahmen bezüglich des betreffenden Produkts ergriffen werden. [Art. 43 Abs. 7 und 8]
- Gibt es hingegen Einwände gegen eine vorläufige Maßnahme, unterzieht die Kommission die vorläufige Maßnahme einer Untersuchung und muss binnen neun Monaten entscheiden, ob sie gerechtfertigt ist oder nicht. Ist sie gerechtfertigt, müssen alle Mitgliedstaaten dafür sorgen, dass das nicht-konforme PmdE vom Markt genommen wird. Ist sie nicht gerechtfertigt, muss der Mitgliedstaat seine Korrekturmaßnahmen zurückziehen. [Art. 44 Abs. 1 und 2]
- Ist die Kommission davon überzeugt, dass ein PmdE, von dem ein erhebliches Cybersicherheitsrisiko ausgeht, die Vorgaben des CRA nicht erfüllt, kann sie eine zuständige Marktüberwachungsbehörde auffordern, eine Bewertung des Produkts vorzunehmen [Art. 45 Abs. 1].
- In Ausnahmefällen, etwa, wenn die relevanten Marktüberwachungsbehörden keine Korrekturmaßnahmen beschlossen haben, kann die Kommission auch die ENISA beauftragen, eine Untersuchung durchzuführen. Basierend auf den Ergebnissen dieser Untersuchung, kann die Kommission Korrekturmaßnahmen beschließen, einschließlich der Anordnung, das betreffende Produkt innerhalb einer angemessenen Frist vom Markt zu nehmen oder zurückzurufen. Eine solche Entscheidung trifft sie durch einen Durchführungsrechtsakt. [Art. 45 Abs. 2–4]
- Marktüberwachungsbehörden können „Sweeps“ durchführen, d.h. koordinierte Kontrollen zur Ermittlung, ob bestimmte PmdE, die häufig Cybersicherheitsrisiken aufweisen, die Anforderungen des CRA erfüllen. Sie werden in der Regel von der Kommission koordiniert. Die ENISA identifiziert Kategorien von PmdE, für die ein Sweep organisiert werden sollte. [Art. 49]

8.2 Sanktionen bei Nichteinhaltung der Vorgaben des CRA

- Die Mitgliedstaaten müssen Vorschriften über Sanktionen für Verstöße von den Wirtschaftsakteuren gegen die Anforderungen erlassen. Die Sanktionen müssen „wirksam, verhältnismäßig und abschreckend“ sein. [Art. 53 Abs. 1]
- Für Verstöße gegen die Sicherheitsanforderungen (Abschnitt 4), die Anforderungen zum Umgang mit Schwachstellen (Abschnitt 5) und gegen die herstellerbezogenen Pflichten gelten Verwaltungsgeldstrafen von bis zu [Art. 53 Abs. 3]
  - 15 Mio. Euro oder
  - 2,5% des weltweiten Gesamtjahresumsatzes des Unternehmens im letzten Geschäftsjahr,

  je nachdem, welcher Betrag höher ist.
- Bei sonstigen Verstößen gelten Verwaltungsgeldstrafen von bis zu
  - 10 Mio. Euro oder
  - 2% weltweiten Gesamtjahresumsatzes des Unternehmens im letzten Geschäftsjahr,

  je nachdem, welcher Betrag höher ist.

9 Zusammenspiel zwischen dem CRA und anderen EU-Rechtsakten

- Der CRA reguliert gezielt den Umgang mit Cybersicherheitsrisiken. PmdE können jedoch auch andere Sicherheitsrisiken bergen. Diese anderen Risiken soll auch weiterhin in der Regel über die Verordnung über die allgemeine Produktsicherheit, die die bestehende Richtlinie zur Produktsicherheit 2001/95/EG zeitnah ersetzen soll, abgedeckt werden. [Erwägungsgrund 28, Art. 7]
- PmdE, die nach der vorgeschlagenen Verordnung über künstliche Intelligenz [KI-Verordnung, COM(2021) 206, s. cep**Analyse**] als Hochrisiko-KI-Systeme eingestuft sind, müssen den Cybersicherheitsanforderungen des CRA genügen. Tun sie dies, kann auch davon ausgegangen werden, dass sie den spezifischen Cybersicherheitsanforderungen der KI-Verordnung genügen [Erwägungsgrund 29, Art. 8].

- Die delegierte Verordnung (EU) 2022/30, die die Richtlinie 2014/53/EU über die Bereitstellung von Funkanlagen auf dem Markt ergänzt, legt für Funkanlagen – z.B. Mobiltelefone, Laptops, Alarmsysteme – grundlegende Anforderungen (1) zum Schutz des Netzes vor Schäden, (2) zum Schutz personenbezogener Daten und der Privatsphäre der Nutzer und sowie (3) zum Schutz vor Betrug, fest. Diese Anforderungen sollen solange gelten bis die horizontalen Cybersicherheitsanforderungen des CRA Anwendung finden. Ab dann sollen die Anforderungen der delegierten Verordnung nicht länger gelten. [Erwägungsgrund 15]
- PmdE, die Maschinenprodukte im Sinne der vorgeschlagenen Maschinenprodukteverordnung [COM(2021) 202] sind, und für die eine EU-Konformitätserklärung nach dem CRA ausgestellt wurde, gelten auch als konform mit den Anforderungen der Maschinenprodukteverordnung in Bezug auf die Sicherheit und Zuverlässigkeit von Steuerungssystemen [Erwägungsgrund 30, Art. 9].
- PmdE, die elektronische Patientendatensysteme (EHR-Systeme) sind und in den Anwendungsbereich der vorgeschlagenen Verordnung über den europäischen Gesundheitsdatenraum [EHDS, COM(2022) 197, s. cep**Analyse**] fallen, müssen auch die Cybersicherheitsanforderungen des CRA erfüllen. Die Konformität der EHR-Systeme sollten sie nach der EHDS-Verordnung nachweisen. [Erwägungsgrund 31, Art. 24 Abs. 4]
- Die Richtlinie über die Haftung fehlerhafter Produkte (85/374/EWG), die derzeit überarbeitet wird [COM(2022) 495] und den Grundsatz festlegt, dass ein Produkthersteller unabhängig vom Verschulden für Schäden haftet, die durch die mangelnde Sicherheit seines Produkts verursacht werden, wirkt ergänzend zum CRA [Erwägungsgrund 16].
- Die Aussteller von „Brieftaschen für die europäische digitale Identität (EUid-Brieftaschen)“ müssen, sofern ihre Brieftaschen gleichzeitig PmdE sind, sowohl die Cybersicherheitsanforderungen des CRA als auch die besonderen Sicherheitsanforderungen der eIDAS-Verordnung [(EU) Nr. 910/2014] erfüllen, die derzeit im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität überarbeitet wird [COM(2020) 281, s. cep**Analyse**] [Erwägungsgrund 18].

10 Geltungsbeginn

- Der CRA gilt 24 Monate nach seinem Inkrafttreten [Art. 57].
- Die Pflicht zur Meldung von Sicherheitsvorfällen und aktiv ausgenutzten Schwachstellen gilt bereits nach 12 Monaten [Art. 57 i.V.m. Art. 11].

B. Juristischer und politischer Kontext

1 Stand der Gesetzgebung

15.09.22 Annahme durch Kommission

Offen Stellungnahme Europäischer Wirtschafts- und Sozialausschuss

Offen Annahme durch Europäisches Parlament und Rat, Veröffentlichung im Amtsblatt, Inkrafttreten

2 Politische Einflussmöglichkeiten

Generaldirektionen:	GD Kommunikationsnetze, Inhalte und Technologien
Ausschüsse des Europäischen Parlaments:	Industrie, Forschung und Energie (ITRE), Berichterstatter: Nicola Danti (Renew, IT)
Bundesministerien:	Inneres (federführend)
Ausschüsse des Deutschen Bundestags:	Inneres (federführend)
Entscheidungsmodus im Rat:	Qualifizierte Mehrheit (Annahme durch 55% der Mitgliedstaaten, die 65% der EU-Bevölkerung ausmachen)

3 Formalien

Kompetenznorm:	Art. 114 AEUV (Binnenmarkt)
Art der Gesetzgebungszuständigkeit:	Geteilte Zuständigkeit (Art. 4 Abs. 2 AEUV)
Verfahrensart:	Art. 294 AEUV (ordentliches Gesetzgebungsverfahren)

C. Bewertung

1 Ökonomische Folgenabschätzung

1.1 Allgemeine Einschätzung

Cyberkriminalität ist weltweit auf dem Vormarsch. Während die Schäden durch Cyberangriffe im Jahr 2015 noch bei rund 2,7 Bio. Euro lagen, haben sie sich bis Ende 2020 mehr als verdoppelt und verursachen mittlerweile Kosten in Höhe von schätzungsweise 5,5 Bio. Euro pro Jahr.[1] Allein die deutsche Wirtschaft kämpft „durch Diebstahl von IT-Ausrüstung und Daten, Spionage und Sabotage“ mit jährlichen Verlusten von ca. 203 Mrd. Euro und rund 84% der deutschen Unternehmen waren 2021 von einer Cyberattacke betroffen.[2] Ein Großteil dieser entstehenden Kosten ist dabei auf unsichere Hard- und Softwareprodukte zurückzuführen. Schwachstellen in diesen Produkten dienen regelmäßig als Ausgangspunkt für Angriffe. Und die Anzahl der Schwachstellen steigt jährlich: Waren es 2020 noch 18.325 sind es 2021 bereits über 20.000.[3] Auch das Bundesamt für die Sicherheit in der Informationstechnik (BSI) vermeldete jüngst einen 10%igen Anstieg der Zahl der Sicherheitslücken in Softwareprodukten für 2021, wobei der Anteil kritischer Schwachstellen – dazu zählten die Lücken in Microsoft Exchange und Log4j (eine Java-Bibliothek) – ca. 13% ausmachte.[4]

---

1 Nai Fovino I., Barry G., Chaudron S., Coisel I., Dewar M., Junklewitz H., Kambourakis G., Kounelis I., Mortara B., Nordvik J.p., Sanchez I. (Eds.), Baldini G., Barrero J., Coisel I., Draper G., Duch-Brown N., Eulaerts O., Geneiatakis D., Joanny G., Kerckhof S., Lewis A., Martin T., Nativi S., Neisse R., Papameletiou D., Ramos J., Reina V., Ruzzante G., Sportiello L., Steri G., Tirendi S., Cybersecurity, our digital anchor, EUR 30276 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-19957-1.

2 Bitkom (2022), Presseinformation, 203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen, 31. August 2022.

3 EU-Kommission (2022), SWD(2022) 282, Impact assessment report, Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, PART 1/3, 15. September 2022, S. 6-8.

4 Bundesamt für Sicherheit in der Informationstechnik (2022), Die Lage der IT-Sicherheit in Deutschland 2022, Oktober 2022.

Diese Entwicklung zeigt auf, dass es den Märkten für Soft- und Hardware offenbar nicht oder nur eingeschränkt gelingt, Produkte hervorzubringen, die als „cybersicher" gelten können. Dies ist auf verschiedene Defizite dieser Märkte zurückzuführen:

Die Hersteller sehen häufig keine Notwendigkeit darin, cybersichere Soft- bzw. Hardwareprodukte zu entwickeln und bereitzustellen. Dies ist darauf zurückzuführen, dass sie für die Schäden, die durch unsichere Produkte entstehen können, regelmäßig nicht (in vollem Umfang) einstehen müssen.[5] Kommt es zu einem Cybersicherheitsvorfall tragen sie nur einen Bruchteil der dadurch entstehenden Kosten. Dazu zählen etwa etwaige Reputationsschäden oder auch Kosten für die Bereitstellung von Sicherheitspatches. Der große Rest muss häufig von den Nutzern der Produkte bzw. von anderen (unbeteiligten) Dritten getragen werden. Damit ist jedoch die Einheit von Handlung und Haftung als konstituierendes Prinzip der Wettbewerbsordnung nicht gegeben. Denn diejenigen Wirtschaftssubjekte, welche als Verursacher bzw. als Verantwortliche für einen Schaden anzusehen sind – hier: die Wirtschaftssubjekte – müssen nicht vollumfänglich für diesen aufkommen. Sie tragen damit nicht die vollen Konsequenzen ihres Handelns.[6] Der Anreiz für die Herstellung von sicheren Soft- bzw. Hardwareprodukts wird zudem dadurch geschmälert, dass die mit Cybervorfällen einhergehenden Reputationsschäden oft nicht von Dauer sind und sich der Nutzer eines Soft- bzw. Hardwareprodukts regelmäßig mit hohen Kosten[7] für einen Wechsel zu einem Konkurrenzprodukt konfrontiert sieht. Die Tatsache, dass die Hersteller Kosten abwälzen können und die Geschädigten hierfür nicht von ihnen kompensiert werden, sorgt damit dafür, dass aus volkswirtschaftlicher Sicht zu wenig Kapital in die Entwicklung von cybersicheren PmdE fließt. Zur Behebung dieses Marktversagens sind also Maßnahmen geboten, die zu einer verstärkten Internalisierung der negativen Externalitäten führen.

Die Märkte für PmdE weisen regelmäßig Charakteristika von „Zitronenmärkten" (Market for lemons) auf. Dies ist darauf zurückzuführen, dass die potenziellen Käufer bzw. Nutzer die cybersicherheitsbezogenen Eigenschaften eines PmdE vor dem Erwerb bzw. der Verwendung häufig nicht oder nur unzureichend einschätzen oder beobachten können. Ihnen mangelt es hierfür an den nötigen Informationen. Haben sie diese jedoch nicht, sind sie auch nicht gewillt, für ein „vermeintlich" cybersicheres Produkt mehr zu bezahlen als für ein anderes Produkt. Dies hat zur Folge, dass diejenigen Hersteller, die tatsächlich sichere Produkte absetzen wollen, aus dem Markt gedrängt werden. Im Endeffekt dominieren langfristig unsichere Produkte, und zwar auch dann, wenn es eigentlich eine Zahlungsbereitschaft für resiliente Produkte gibt. Die asymmetrische Informationsverteilung zwischen Herstellern und Käufern/Nutzern führt also zu einer „adversen Selektion", die keine hinreichend sicheren PmdE hervorbringt.[8,9]

Die Märkte für PmdE sind häufig von Netzwerkeffekten, von Größenvorteilen und von einer hohen Innovationsfreudigkeit und kurzen Innovationszyklen geprägt. Diese Faktoren führen dazu, dass die Hersteller in der Regel ein großes Interesse daran haben, ihr PmdE zügig in Verkehr zu bringen. Aufwändige und kostenintensive Investitionen in die Verbesserung der Cybersicherheit ihrer Produkte – eine Produkteigenschaft, die bei der Kaufentscheidung häufig nicht an erster Stelle steht – verzögern den Markteintritt und können sich daher nachtteilig im Wettbewerb auswirken. Auch diese Faktoren sorgen somit dafür, dass sich tendenziell weniger sichere PmdE am Markt etablieren.[10]

Auch auf Seiten der Käufer bzw. Nutzer von PmdE können Fehlanreize vorherrschen, die zu Trittbrettfahrerverhalten einladen. Generell ist der Erwerb eines cybersicheren PmdE mit positiven Externalitäten verbunden. Nicht nur der Käufer profitiert von dem sicheren Produkt, sondern auch Dritte, da das allgemeine Cybersicherheitsniveau steigt. Die profitierenden Dritten leisten jedoch für diesen Zusatzgewinn an Sicherheit keinen eigenen Beitrag. Zudem schmälert es ihre Notwendigkeit, selbst in die Cybersicherheit investieren zu müssen. Beide Effekte

---

5 Moore, T. (2010), The economics of cybersecurity: Principles and policy options. International Journal of Critical Infrastructure Protection, 3(3-4), S. 5 und 6.

6 Eucken, W. (1952/2004), Grundsätze der Wirtschaftspolitik, Mohr Siebeck, Tübingen.

7 Diese können teilweise auch sehr hoch sein, etwa wenn kein gleichwertiges Substitutsprodukt zur Verfügung steht.

8 Kox, H., & Straathof, B. (2014), Economic aspects of Internet security. *CPB Background Document*, S. 13 und 14.

9 Mohaddes Deylami, H., Ardekani, I., Muniyandi, R. C., & Sarrafzadeh, H. (2015). Effects of software security on software development life cycle and related security issues, S. 5.

10 Asghari, H., van Eeten, M., & Bauer, J. M. (2016). Economics of cybersecurity. Handbook on the Economics of the Internet.

führen jedoch schlussendlich dazu, dass der Anreiz überhaupt in cybersichere Produkte zu investieren, gering ausfallen kann.[11]

All dies sorgt dafür, dass die Hersteller tendenziell PmdE auf den Markt bringen, die nicht hinreichend cybersicher sind und die Kunden bzw. Nutzer gleichzeitig auch keine hinreichend sicheren Produkte nachfragen (können). Es ist also durchaus geboten hier Abhilfe zu schaffen. Das Cyberresilienzgesetz leistet hierfür einen wichtigen Beitrag:

1.2 Festlegung einheitlicher Cybersicherheitsanforderungen

Die Verpflichtung für Hersteller, Einführer und Händler von PmdE, grundlegende Cybersicherheitsanforderungen erfüllen zu müssen und dafür zu sorgen, dass die Cybersicherheit bereits in der Konzeption, Entwicklung und Herstellung eines Produkts mitbedacht werden muss, wirkt drei der vier oben beschriebenen Marktdefizite entgegen.

Erstens kann Fehlanreizen auf Seiten der Wirtschaftsakteure wirksam vorgebeugt werden. So müssen sie mehr in die Cybersicherheit ihrer Produkte investieren, was potenziell die Schäden bzw. Kosten, die ihre Kunden bzw. (unbeteiligte) Dritte aufgrund unsicherer PmdE tragen müssen, reduziert. Handlung und Haftung werden wieder verstärkt in Einklang gebracht und die Möglichkeiten zur Abwälzung von Kosten reduziert. Die zusätzlichen Pflichten sorgen somit für eine gewisse Internalisierung negativer (Netzwerk-)Externalitäten.

Zweitens schaffen harmonisierte Cybersicherheitsanforderungen einheitliche Wettbewerbsbedingungen und es entstehen nicht länger potenzielle Nachteile im Markt für jene Wirtschaftsakteure, die proaktiv sichere Produkte bereitstellen und aufgrund dessen beispielsweise verspätet mit ihrem Produkt in den Markt eintreten. Cybersicherheit als wesentliches Grundelement eines PmdE kann nicht länger, etwa aufgrund höherer Produktionskosten oder eines verspäteten Markteintritts vom Markt bestraft werden, sondern wird als zentraler Wettbewerbsfaktor etabliert.

Drittens beugen einheitliche Cybersicherheitsanforderungen Trittbrettfahrerverhalten auf Seiten der Käufer von PmdE vor. Sie können sich nun zwar sicher sein, dass andere Käufer auch cybersichere Produkte erwerben bzw. erworben haben und damit von positiven Externalitäten profitieren. Gleichzeitig können sie sich jedoch nicht länger aus der Verantwortung für ein cybersicheres Umfeld herausstehlen, da weniger „unsichere“ Produkte zur Verfügung stehen werden.

1.3 Rückgriff auf das New Legislative Framework

Zahlreiche Produkte, die in der EU auf den Markt gebracht werden, müssen hierfür bestimmte Sicherheits-, Gesundheits- oder Umweltanforderungen erfüllen. Dabei wird auf das New Legislative Framework (NFL) zurückgegriffen, welches Grundregeln für die Produktregulierung in der EU festlegt.[12] Es funktioniert nach dem Grundsatz, wonach Produkte bestimmte Sicherheitsziele erreichen müssen, bevor sie in Verkehr gebracht werden können, ohne jedoch technisch en détail festzulegen, wie diese Ziele zu erreichen sind.[13] Es basiert insbesondere auf der Bewertung der Konformität der Produkte mit den jeweiligen Anforderungen durch die Hersteller selbst oder durch Dritte, einer Marktüberwachung durch Aufsichtsbehörden, einer technischen Dokumentation der Eigenschaften des Produkts und der CE-Kennzeichnung. Dass die Kommission auch beim CRA auf dieses, seit 2010 geltende Rahmenwerk zurückgreift, erleichtert die Umsetzung der umfangreichen Cybersicherheitsanforderungen enorm. Denn die Hersteller von PmdE sind vielfach, abseits von einigen Softwareentwicklern[14], bereits damit vertraut, und können daher auf etablierten Verfahren und Prozessen aufsetzen.

---

11 Kox, H., & Straathof, B. (2014), S. 26.

12 Auf Basis des NLF wurden bisher Rechtsakte für zahlreiche in der EU vermarktete Produkte erlassen. Dies betrifft mittlerweile mehr als 20 Sektoren. Dazu zählen etwa elektrotechnische Produkte, Spielzeug und Medizinprodukte [SWD(2022) 282, PART 2/3, Annex 11].

13 EU-Kommission (2016), Leitfaden für die Umsetzung der Produktvorschriften der EU 2016 („Blue Guide“), C/2016/1958.

14 Dies liegt daran, dass Software bisher häufig nicht als Produkt gilt und es für sie daher auch bisher kaum Produktanforderungen nach dem NFL gibt.

1.4 Anwendungsbereich

Dass die Kommission für die Cybersicherheitsanforderungen einen sehr breiten Anwendungsbereich wählt und dabei neben Hardwareprodukten sowohl nicht-eingebettete als auch eingebettete Software und auch Komponenten einbezieht, ist sachgerecht, auch wenn damit eine Fülle von Wirtschaftsakteuren und insbesondere kleine und mittlere Unternehmen (KMU) vor großen Herausforderungen stehen werden.[15] Denn Sicherheitslücken in PmdE sind kein Phänomen, das auf bestimmte Produkte bzw. produktarten/-kategorien beschränkt ist. Zudem können auch PmdE, die eigentlich als unkritisch gelten und in vermeintlich sicheren Umgebungen eingesetzt werden, als Einfallstor dienen und zu einer raschen Verbreitung einer Schwachstelle beitragen. Ferner ist vor dem Inverkehrbringen eines PmdE häufig nicht eindeutig absehbar, von wem, zu welchen Zwecken und in welchem Umfeld dieses eingesetzt wird. Einheitliche Mindestvorgaben für alle PmdE, unabhängig von ihrer Kritikalität, können daher zu einer spürbaren Erhöhung des Cybersicherheitsniveaus beitragen. Gleichwohl sollten besonders zwei Aspekte bedacht werden. Erstens sind ein Großteil (über 90%) der Hersteller von PmdE KMU, die, insbesondere wenn sie Softwareprodukte entwickeln, bisher nicht mit den vorgeschriebenen Produktprüfungsprozessen, inklusive der Konformitätsbewertung, vertraut sind. Dass insbesondere diese KMU sich binnen zwei Jahren auf diese Verfahren in zufriedenstellender Weise einstellen und spezifisches Knowhow aufbauen können, ist unrealistisch. Hier sollte über eine längere Implementierungsfrist nachgedacht werden, zumindest für solche Produktkategorien, die als weniger kritisch erachtet werden. Zweitens sollte der Umgang mit kommerzieller Open-Source Software nochmals überdacht werden. Zwar ist auch deren Sicherheit zentral für cyberresiliente europäische Volkswirtschaften. Da deren Entwicklung jedoch meist nur auf den Schultern weniger Personen lastet, die zudem häufig freiwillig erfolgt und mit wenig Kapital auskommen muss, würden teure Produktprüfungsverfahren vielfach dazu führen, dass ihre Entwicklung sich ggfs. nicht länger rechnet. Da gleichzeitig viele Softwareprodukte auf Open-Source-Produkten aufbaut, bestünde die Gefahr, dass die Softwareentwicklung in der EU zumindest ins Stottern geraten könnte. Daher gilt es im weiteren Gesetzgebungsprozess eine Balance zwischen dem berechtigten Wunsch nach einem höheren Cybersicherheitsniveau und der Aufrechterhaltung von Anreizen zur Entwicklung von freier, quelloffener Software zu finden.

Dass die Kommission eine Abstufung der Regulierungstiefe abhängig von der Kritikalität des Produkts vornimmt und für „kritischere“ Produkte strengere Verfahren zur Konformitätsbewertung vorschreibt, ist im Grundsatz sachgerecht und stärkt die Resilienz gegenüber Cybervorfällen zusätzlich. Jedoch sind sowohl das Verfahren zur Einstufung der PmdE als auch die Einstufung an sich fragwürdig:

Erstens ist die bereits von der Kommission vorgenommene Einstufung von Produkten in die Klassen 1 und 2 für kritische Produkte undurchsichtig. So ist insbesondere nicht klar, welche Kriterien sie für die Einordnung in die beiden Gruppen herangezogen hat und worin genau die Unterscheidung zwischen einem Klasse 1- und einem Klasse 2-Produkt besteht, obgleich die Eingruppierung reale Folgen, insbesondere hinsichtlich der Strenge der Konformitätsbewertung zeitigt. Sollten bereits im Primärrechtsakt bestimmte PmdE als kritische Produkte festgelegt und in verschiedene Risikoklassen eingeteilt werden, bedarf es hierfür jedenfalls einer gründlicheren Untermauerung.

Zweitens gehen mit dem Recht, das der Kommission zur Festlegung weiterer kritischer Produkte eingeräumt wird, veritable Rechtunsicherheiten einher. Zwar werden ihr verschiedene Kriterien, wie etwa die Prüfung der Cyberfunktionalität des PmdE oder das Ausmaß von Verlusten oder Störungen, die durch den Einsatz eines PmdE bereits entstanden sind, mit an die Hand gegeben. Das ist zielführend, um willkürliche Entscheidungen zu verhindern. Es wird anhand der Vorgaben jedoch nicht ersichtlich, welche Faktoren für die Eingruppierung als Klasse 1 vs. Klasse 2 entscheidend sind und ob den Kriterien eine unterschiedliche Gewichtung eingeräumt wird. Dies sollte präzisiert werden.

Drittens ist die Einstufung nicht schlüssig. Denn vielfach sind die PmdE in den beiden Klassen nicht per se und unter allen Umständen als kritisch anzusehen. Ihre Kritikalität steht und fällt stattdessen insbesondere damit, von wem, unter welchen Bedingungen und in welchen (sensiblen) Umgebungen sie eingesetzt werden. So kann bspw. der Einsatz der PmdE durch kritische Infrastrukturbetreiber bei der Erbringung ihrer spezifischen Dienstleistungen zumindest als ein Indikator dafür dienen, dass verstärkte Vorsicht geboten ist. Und auch, wenn eine Störung oder der Ausfall des PmdE massive Auswirkungen für das Funktionieren des Gemeinwesens haben

[15] Laut Kommission lag die Zahl der Unternehmen im Softwaremarkt in der EU im Jahr 2019 bei ca. 366.000. Über 99% davon waren KMU. Die Zahl der Hardwareproduktehersteller lag im selben Jahr bei ca. 22.800. Auch diese sind mit über 97% überwiegend KMU [SWD(2022) 282, PART 2/3, S. 24 und 25].

könnte, sollte dies ein Signal dafür sein, strengere Anforderungen an ihre Cybersicherheit zu stellen. Wird ein PmdE jedoch in einem weniger kritischen Umfeld genutzt, ist es nicht zwingend gleich als „kritisch“ einzustufen. Die Einteilung der PmdE in Kritikalitätsstufen sollte daher viel stärker noch auf diese Faktoren abstellen. Damit würde der mit den Cybersicherheitsanforderungen einhergehen Aufwand für die Hersteller der PmdE gesenkt, ohne gleichzeitig wesentliche Abstriche bei der Erhöhung der Cyberresilienz zu machen.

1.5 Perspektive Produktlebenszyklus

Üblicherweise fokussiert der NFL auf die Vorgabe von Produktanforderungen, die vor dem Inverkehrbringen eines Produkts zu erfüllen sind. Ob dieses auch im Anschluss Anforderungen etwa an seine Sicherheit erfüllt, ist zweitrangig. Der CRA nimmt nun bezüglich der Cybersicherheit von PmdE eine Perspektive ein, die den ganzen Produktlebenszyklus der Produkte in den Blick nimmt. Der Hersteller eines PmdE trägt demnach auch dann noch Verantwortung für sein Produkt, wenn dieses bereits verwendet wird. Das ist auch der richtige Weg. Denn erstens treten Cyberrisiken regelmäßig auch während der Nutzungsphase eines PmdE in Erscheinung, die ex ante nicht oder nur schwer zu antizipieren sind. Auch mit den größten Anstrengungen kann ein Hersteller nicht ausschließen, dass sein Produkt eine Schwachstelle aufweist. Zweitens werden insbesondere Softwareprodukte häufig während ihrer Lebensdauer mit neuen Features ausgestattet, die neue Risiken bergen können, die entsprechend ex post (also nach dem Inverkehrbringen) zu adressieren sind. Der Lebenszyklusansatz reduziert damit Fehlanreize auf Seiten der Produkthersteller und wirkt damit einhergehenden Marktdefiziten entgegen.

1.6 Schwachstellenmanagement

Der begrüßenswerte Lebenszyklusansatz inkludiert auch die Pflicht zur Behandlung und Behebung von Schwachstellen – u.a. durch Sicherheitsaktualisierungen – über die erwartete Produktlebensdauer des PmdE bzw. über fünf Jahre ab dem Inverkehrbringen des Produkts, je nachdem, welcher Zeitraum kürzer ist. Damit wird für Hersteller genau festgelegt, für wie lange sie sich verpflichtend mit der Cybersicherheit ihrer Produkte beschäftigen müssen. Das schafft erstens Rechtssicherheit auf Seiten der Hersteller, erhöht zweitens das Vertrauen der Nutzer in die Produktqualität und stellt drittens sicher, dass das Interesse der Hersteller an der Cybersicherheit auch nach dem Inverkehrbringen nicht zu schnell schwindet. Fünf Jahre als maximale Frist für die Pflicht zur Schwachstellenbehandlung bilden dabei einen gut austarierten Kompromiss. Er stellt sicher, dass zwar für einen gewissen Zeitraum Ressourcen zur Festigung der Sicherheit „alter“ Produkte bei Herstellern gebunden sind, diese Bindung jedoch nicht gleichzeitig dazu führt, dass Produktinnovationen ausbleiben bzw. der Anreiz auf neuere PmdE umzusteigen, die ein höheres Sicherheitsniveau versprechen, unterminiert wird. Auch verhindert die 5-Jahres-Frist, dass Hersteller langfristig unnötige Ressourcen dafür einsetzen müssen, PmdE auf dem neuesten Stand zu halten, obgleich diese sich überhaupt nicht am Markt durchgesetzt haben.

Im weiteren Verhandlungsprozess sollten jedoch noch Klarstellungen vorgenommen werden, wie der Begriff der „erwarteten Lebensdauer“ zu verstehen ist. Während dies bei einem physischen PmdE eindeutig und einfach festlegbar bzw. bestimmbar erscheint, ist dies insbesondere bei Softwareprodukten nicht immer der Fall. Denn bei diesen Produkten stellt sich regelmäßig die Frage, ob eine neue Softwareversion nur ein Update der „alten“ Software ist oder ein Upgrade, sodass letztlich ein „neues“ Softwareprodukt in Verkehr gebracht wird und die Produktlebensdauer der alten Software damit endet. Diesbezügliche Klarstellungen würden jedenfalls dazu beitragen, die Rechtssicherheit für Hersteller zu erhöhen. Sie könnten etwa darauf abstellen, ob das Softwareprodukt in „wesentlichem Umfang“ verändert wird. Des Weiteren sollte Kohärenz zu anderen EU-Rechtsakten sichergestellt sein, um widersprüchlichen Regelungen vorzubeugen. So könnten die von der Kommission kürzlich im Rahmen ihres Vorschlags für eine Richtlinie zur Haftung für fehlerhafte Produkte [COM(2022) 495] vorgelegten Vorschriften beispielsweise so interpretiert werden, dass Updates für bis zu zehn Jahren bereitgestellt werden müssen und damit deutlich länger als es der CRA Vorschlag vorgibt. Und auch kürzlich vorgestellte neue Ökodesignvorgaben[16], die für Smartphones, Tablets und Mobiltelefone gelten sollen, sehen beispielsweise vor, dass Hersteller bzw. Einführer dieser Produkte auch noch bis zu 5 Jahre, nachdem ein solches Produkt vom Markt genommen wurde, Sicherheits-, Korrektur- und Funktionsupdates für das verwendete Betriebssystem kostenlos bereitstellen müssen, wodurch ein Gleichklang mit den Vorgaben des CRA nicht gegeben ist.

[16] BMUV und BMWK (2022): Smartphones und Tablets sind zukünftig leichter reparierbar, Pressemitteilung Nr. 161/22, Konsum und Produkte, 18.11.2022.

1.7 Auslieferung ohne bekannte Schwachstellen

Der CRA Vorschlag verpflichtet Hersteller dazu, nur PmdE auszuliefern, bei denen zum Zeitpunkt des Inverkehrbringens keine „ausnutzbare Schwachstelle“ bekannt ist. Ist eine solche bekannt, darf das Produkt nicht ausgeliefert werden. Die Vorgabe ist an sich schlüssig, sorgt sie doch dafür, dass die Hersteller ernsthaft darum bemühen müssen, nur cybersichere Produkte auf den Markt zu bringen und beugt damit auch dem Fehlanreiz entgegen, etwa aus Innovationsgründen, ein Produkt möglichst zügig zu vermarkten, obgleich dessen Cybersicherheit nicht gegeben ist. Die Vorschrift sollte dennoch nachgeschärft werden. Denn es ist zu bezweifeln, dass ein Hersteller zum Zeitpunkt des Inverkehrbringens vollumfänglich garantieren kann, dass sein Produkt keine dieser Schwachstellen enthält, insbesondere auch, da zwischen der Finalisierung des Herstellungsprozesses und der Auslieferung – besonders bei Hardwareprodukte – eine gewisses zeitliche Lücke bestehen dürfte. Ferner sollte nicht jegliche bekannte und ausnutzbare Schwachstelle dazu führen müssen, den Auslieferungsprozess zu verschieben, sondern nur solche, von denen ein gewisses Sicherheitsrisiko ausgeht bzw. auszugehen droht. Ansonsten drohen unnötige und leicht vermeidbare Verzögerungen beim Markteintritt. Eine zielführende Regelung wäre demnach eine, die sichergestellt, dass die Hersteller „angemessene“ Anstrengungen unternehmen müssen, dass ihr Produkt möglichst schwachstellenfrei in Verkehr gebracht wird. Sie sollten hierbei jedoch risikoorientiert vorgehen und sich auf die schwerwiegenden Sicherheitslücken konzentrieren dürfen.

1.8 Transparenzvorgaben

Die Festlegung von Transparenzvorgaben, etwa darüber, unter welchen Umständen bei der Nutzung des Produkts Cybersicherheitsrisiken eintreten könnten oder darüber, wie lange der Nutzer mit Sicherheitsupdates rechnen kann, versetzt Verbraucher und Unternehmen in die Lage, die Sicherheitseigenschaften von PmdE besser einordnen und vergleichen zu können, und befähigt sie dazu eine fundierte Entscheidung über den Erwerb eines PmdE fällen zu können. Sie sind damit ein wesentlicher Baustein bei der Abwendung von durch Informationsasymmetrien bedingten Marktversagen, ein zentrales Element bei der Sicherstellung eines effektiven Wettbewerbs zwischen den PmdE-Herstellern und letztlich zur Herausbildung eines Marktes für cybersichere PmdE.

1.9 Meldepflichten

Wie auch bereits die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS 2-Richtlinie, s. cep**Adhoc**) und die Verordnung über die digitale Betriebsstabilität (DORA, s. cep**Analyse**) etabliert auch der CRA Meldepflichten beim Auftreten von Sicherheitsvorfällen bzw. hier auch für auftretende Schwachstellen bei den PmdE. Hersteller von PmdE haben häufig kein Eigeninteresse daran, Vorfälle oder Schwachstellen freiwillig zu melden, da hiermit Reputationsschäden einhergehen und Vertrauensverluste entstehen können. Gleichzeitig haben solche Meldungen häufig einen hohen volkswirtschaftlichen Nutzen, da (unbeteiligte) Dritte sich rascher auf eine neue Gefahrenlage einstellen und frühzeitiger Maßnahmen zur Reduktion von Risiken treffen können. Meldepflichten sind daher grundsätzlich sachgerecht, insbesondere auch, da sie Anreize für Hersteller schaffen, schon im Vorfeld in die Sicherheit ihrer PmdE zu investieren. Die avisierten Meldepflichten des CRA sind jedoch aus drei Gründen verbesserungswürdig. Erstens ist die Pflicht zur Notifizierung jedweder ausnutzbaren Schwachstelle bzw. jedwedes Sicherheitsvorfalls[17] überschießend. Dies bindet unnötigerweise Ressourcen, ohne einen großen Mehrwert zu generieren und bedeutet, dass PmdE-Hersteller in letzter Konsequenz strengeren Meldepflichten unterliegen als die Betreiber kritischer Infrastrukturen. Analog zur NIS 2-Richtlinie sollte hier auf die Signifikanz des Vorfalls bzw. der Schwachstelle abgestellt werden. Zweitens erscheint eine einmalige Meldung bereits nach nicht mal 24 Stunden unzureichend. Eine solch kurzfristige Notifizierung kann immer nur erste rudimentäre Informationen enthalten, mit denen jedoch sowohl die Aufsichtsbehörden, inklusive der ENISA, die Kunden und andere Dritte oft noch nicht viel anfangen können. Eine solche Erstmeldung kann letztlich zunächst nur ein Warnhinweis sein. Auf diese sollte daher zu einem späteren Zeitpunkt noch weitere Meldungen mit mehr Detailinformationen, ggfs. in Anlehnung an die Regelungen der NIS 2-Richtlinie, folgen. Und drittens sollte sichergestellt werden, dass die Hersteller der PmdE nicht zu Mehrfachmeldungen an mehrere verschiedene Adressaten gezwungen werden. Dies könnte etwa dann eintreten, wenn ein PmdE-Hersteller gleichzeitig auch eine wesentliche oder wichtige Einrichtung im Sinne der NIS 2-Richtlinie, also etwa ein Energieversorgungsunternehmen, ist. In diesem Fall wäre er ggfs. gezwungen, einen Cybersicherheitsvorfall mehreren

[17] Auffallend ist ferner, dass es dem Kommissionsvorschlag an einer Definition des Begriffs „Sicherheitsvorfall“ mangelt. Eine solche Definition findet sich jedoch in Artikel 4 der NIS 2-Richtlinie.

Stellen zu melden, nämlich der ENISA und der nationalen Aufsichtsbehörde bzw. einem nationalen CSIRT.[18] Um den Meldeaufwand für die betroffenen Unternehmen zu senken, sollte in solchen Fällen eine einzige Meldestelle genügen, welche die Notifizierungen anschließend wiederum an jene weiteren Stellen weiterleitet, die die Informationen benötigen. Des Weiteren ist die Pflicht zur Information von Nutzern über jegliche Sicherheitsvorfälle zu weitgehend. Hier sollte der Fokus ebenfalls auf deren Signifikanz sowie auf deren direkten Auswirkungen für die Nutzer des PmdE gerichtet werden.

1.10 Konformitätsbewertung

Konformitätsbewertungen sind ein bewährtes Verfahren des NLF durch das die Hersteller nachweisen können, dass ihre Produkte gewissen Produktanforderungen auch tatsächlich genügen. Sie sind ein zentrales Element zur Stärkung in das Vertrauen in die Sicherheit von Produkten und ein weiteres Instrument zur Reduktion von Fehlanreizen auf Seiten der Produkthersteller. Der Rückgriff auf die bereits lange etablierten Bewertungsverfahren auch für die Prüfung der Cybersicherheit von PmdE ist dabei zielführend. Dass die Kommission ferner einen risikobasierten Ansatz verfolgt, der für den Großteil der PmdE (ca. 90% laut Kommission) eine Selbstbewertung durch den Hersteller erlaubt und nur für kritische Produkte[19] (ca. 10% laut Kommission) eine strengere Bewertung unter Hinzuziehung von unabhängigen dritten Stellen vorsieht, ermöglicht dabei eine effiziente Verteilung begrenzter Ressourcen und beugt einer Überlastung von Herstellern, Konformitätsbewertungsstellen und Aufsichtsbehörden vor.

Die Kommission will es Herstellern ermöglichen, im Rahmen der Konformitätsbewertung insbesondere auf harmonisierte EU-Standards zurückzugreifen, die die grundlegenden und nicht auf ein bestimmtes Produkt oder eine bestimmte Technologie abzielenden Cybersicherheitsanforderungen des CRA Vorschlags konkretisieren. Das ist zielführend, denn die Anwendung der in diesen Standards verankerten produktspezifischen technischen Detailanforderungen erleichtert es den Herstellern die Konformität ihrer Produkte nachzuweisen enorm. Dies senkt den Aufwand für die Befolgung der Vorschriften deutlich, erhöht die Rechtssicherheit für Hersteller und sorgt für eine einheitliche Anwendung der Rechtsvorschriften. Die Verwendung etwa von technischen Spezifikationen oder sonstigen Lösungen ist regelmäßig mit größerem Aufwand auf Seiten der Produkthersteller verbunden und mit größeren Unsicherheiten verbunden. Es ist jedoch fraglich, ob der Rückgriff auf die harmonisierten EU-Standard zum Zeitpunkt der Erstanwendung der Verordnung gelingen wird. Denn es ist wenig realistisch, dass die Kommission gemeinsam mit den einschlägigen Normungsorganisationen und -gremien in der Lage sein werden, die notwendigen Standards binnen zwei Jahren für eine so große Anzahl von PmdE auszuarbeiten und rechtzeitig zu finalisieren. Es wäre daher überlegenswert, die Ersterfüllung der Cybersicherheitsanforderungen der Verordnung enger an das tatsächliche Vorliegen der EU-Standards zu koppeln. Eine solche Kopplung sollte jedoch nicht dazu verleiten, den Normungsprozess und letztlich die Erfüllung der Vorgaben des CRA unnötig zu verzögern.

1.11 Marktüberwachung

Einheitliche, sektorübergreifende Cybersicherheitsanforderungen für PmdE sind nur wirksam, solange sichergestellt ist, dass diese von den betroffenen Wirtschaftsakteuren auch tatsächlich umgesetzt und gelebt werden. Hierfür ist eine Marktüberwachung essenziell, die sicherstellt, dass PmdE, die als nicht cybersicher gelten, nicht im EU-Binnenmarkt zirkulieren dürfen. Dass die Kommission hierfür auf das bestehende, austarierte System im Rahmen des NLF setzt, ist zielführend. Denn das Marktüberwachungsregime stellt insbesondere sicher, dass PmdE, die von einer nationalen Marktaufsichtsbehörde als nicht cybersicher angesehen werden, im gesamten EU-Binnenmarkt nicht mehr in Verkehr gebracht werden dürfen bzw. aus dem Verkehr gezogen werden müssen. Das sorgt für ein einheitliches Schutzniveau innerhalb der EU, wirkt Wettbewerbsverzerrungen und uneinheitlichen Handelsbedingungen entgegen und schafft Anreize auf Seiten der Hersteller die Cybersicherheit der Produkte im Rahmen der Produktgestaltung und -entwicklung proaktiv zu berücksichtigen. Für letzteres sorgen zudem die durchaus abschreckenden Sanktionsregelungen. Sollte dennoch, etwa aufgrund mangelnder Ressourcen oder etwaiger Interessenkonflikte, eine nationale Marktüberwachungsbehörde seine Aufgaben nicht in angemessener Weise ausüben (können), bietet der Umweg über ein Eingreifen der Kommission – in Zusammenarbeit

---

[18] Kommt es bei einem Sicherheitsvorfall zudem zu einer Verletzung des Schutzes personenbezogener Daten, muss der Verantwortliche dies nach Artikel 33 der Datenschutzgrundverordnung (DSGVO) spätestens binnen 72 Stunden der zuständigen Datenschutzaufsichtsbehörde melden; d.h. hier gibt es potenziell einen weiteren Adressaten, an den Meldungen übermittelt werden müssen und erneut eine andere Frist für Notifizierungen.

[19] Wie oben bereits angemerkt, sollte jedoch die Einteilung von PmdE in die verschiedenen Risikogruppen nochmals überdacht werden.

mit der ENISA – im Ausnahmefall einzugreifen und produktspezifische Abhilfemaßnahmen festzulegen, einen zusätzlichen Schutz, der die Cyberresilienz in der EU stärken kann.

1.12 Geltungsbeginn:

Der Kommissionsvorschlag sieht vor, dass der CRA bereits zwei Jahre nach seinem Inkrafttreten gelten soll. Dieser Zeitplan ist aufgrund der hohen Gefahrenlage und den wirtschaftlichen Schäden durch Cyberattacken durchaus nachvollziehbar. Je früher PmdE cybersicher(er) sind, desto besser. Gleichwohl erscheint der Zeitplan, trotz der Dringlichkeit der Problematik, als zu ambitioniert und sollte daher überdacht werden. Denn erstens ist nicht zu erwarten, dass sowohl auf Seiten der Hersteller als auch auf Seiten der Prüfinstanzen und Aufsichtsbehörden in diesem kurzen Zeitfenster genügend Expertise, Knowhow und Personal aufgebaut werden kann, um eine adäquate Erfüllung, Prüfung und Überwachung der Cybersicherheitsanforderungen gewährleisten zu können. Man bedenke, dass die Zahl der erfassten Hardware- und Softwareprodukte äußerst umfangreich ist und, auch wenn nicht mehr als 10% der PmdE als kritische Produkte gelten und damit strengeren Konformitätsbewertungen unterliegen sollen, sind dies dennoch nicht gerade wenige. Zweitens sind über 90% der Hersteller KMU oder gar Mikrounternehmen, die wenn sie Softwareentwickler sind, kaum oder überhaupt nicht mit Pflichten zu Produktanforderungen vertraut sind. Und drittens ist nicht sicher, dass (europäische) Normen und technische Spezifikationen zu bestimmten Produkten oder Produktkategorien zeitnah in einem Ausmaß vorliegen werden, die eine sachgemäße Konformitätsbewertung ermöglichen. Aus den genannten Gründen wäre ein späterer Geltungsbeginn daher geboten. Ggfs. sollte über eine gestaffelte Implementierung nachgedacht werden, bei der die CRA-Anforderungen für PmdE, die in kritischen Bereichen, etwa von kritischen Infrastrukturbetreibern, eingesetzt werden, früher gelten als für andere PmdE. Dies würde auch einer möglichen Überlastung der beteiligten Akteure kurz vor Beginn der Anwendungsphase des CRA entgegenwirken.

2 Juristische Bewertung

2.1 Kompetenz

Der CRA wird auf die Rechtsgrundlage der Rechtsangleichung im Binnenmarkt [Art. 114 AEUV] gestützt. Nach diesem Artikel darf die EU die Maßnahmen zur Weiterentwicklung des Binnenmarkts ergreifen. Der CRA zielt darauf ab, den freien Warenverkehr von Produkten mit digitalen Elementen zu ermöglichen, indem es harmonisierte Cybersicherheitsanforderungen für diese Produkte in allen Mitgliedstaaten festlegt. Der Gegenstand und das Ziel der Verordnung entsprechen den Voraussetzungen des Art. 114 AEUV. Die Kompetenz ist daher gegeben.

2.2 Subsidiarität und Verhältnismäßigkeit gegenüber den Mitgliedstaaten

Der Handel mit PmdE hat häufig grenzüberschreitenden Charakter. Auch in die EU importierte PmdE werden zumeist nicht nur in einem oder wenigen Mitgliedstaaten vertrieben. Überdies werden bei den PmdE oft die Datenfernverarbeitungs- und Netzlösungen verwendet, sodass es nicht möglich ist, die Verwendung des Produktes geographisch einzugrenzen oder zu beschränken. Technische Möglichkeiten lassen sekundenschnell Daten auf andere Geräte übertragen sowie Verbindungen zwischen elektronischen Komponenten und Systemen ohne physischen Kontakt mit dem Gerät herstellen. Infolgedessen droht ein geringes Niveau an Cybersicherheit sogar in einem Element mit weitgehenden Auswirkungen. Aktiv ausgenutzte Cybersicherheitsschwachstellen und Sicherheitsvorfälle können Einfluss auf mehrere Mitgliedstaaten oder sogar auf den gesamten Binnenmarkt haben, deswegen ist eine EU-weite Regulierung sinnvoll.[20]

Aufgrund der blitzschnellen Verbreitung der Daten zwischen PmdE in entfernte Teile der Welt, rufen unterschiedliche nationale Rechtsvorschriften sowie vorhandene Gesetzeslücken Rechtsunsicherheiten und rechtliche Hindernisse hervor. Da eine räumliche Abgrenzung der Verwendung von PmdE kaum möglich und kontraproduktiv wäre, spricht dies gegen die Einführung von Maßnahmen einzelner EU-Mitgliedstaaten. Für einen effektiven und offenen Binnenmarkt sind einheitliche Rechtsnormen für alle in der EU in Verkehr gebrachte PmdE notwendig. Mit anderen Maßnahmen wie etwa nichtlegislativen Vorhaben kann kein annähernd hohes Niveau an Cyberresilienz erreicht werden, wie es durch einen verbindlichen Rechtsakt wie den CRA möglich ist und wäre daher

[20] Urteil des Gerichtshofes (Große Kammer) vom 2. Mai 2006, Vereinigtes Königreich Großbritannien und Nordirland gegen Europäisches Parlament und Rat der Europäischen Union, Rechtssache C-217/04, Rn. 63.

weniger effektiv. Daher stellt der Erlass einer Verordnung auf supranationaler eine optimale Lösung dar. Vor diesem Hintergrund sind Subsidiarität und Verhältnismäßigkeit gegenüber den Mitgliedstaaten unproblematisch.

Nichtdestotrotz kann die Verhältnismäßigkeit einiger Vorschriften angezweifelt werden. Auf den ersten Blick kann der vorgesehene Geltungsbeginn des CRA als verspätet vorkommen, da der Notwendigkeit, die Cybersicherheit zu stärken, schon heute besteht und auch in den zwei Jahren bis zum Anwendungsbeginn des CRA mehrere Sicherheitsvorfälle auftreten können und Schwachstellen entdeckt werden können, auch aufgrund fehlender Maßnahmen seitens der Hersteller von PmdE und der anderen beteiligten Wirtschaftsakteure. Allerdings kann die Anpassung und Einführung notwendiger Maßnahmen, um die zahlreichen Anforderungen des CRA erfüllen zu können, eine Herausforderung darstellen, insbesondere für die Hersteller, die jahrelange Entwicklungszyklen für ihre PmdE haben.

2.3 Sonstige Vereinbarkeit mit EU-Recht

Nach dem CRA Vorschlag darf die Kommission mittels delegierter Rechtsakte den CRA in bestimmten Teilen ändern oder ergänzen. Nach Art. 290 AEUV darf die Kommission Rechtsakte ohne Gesetzescharakter erlassen, um nicht wesentliche Aspekte eines Gesetzgebungsaktes zu ändern oder den Gesetzgebungsakt, um nicht wesentliche Elemente zu ergänzen. In dem Artikel ist jedoch nicht klar geregelt, welche Teile eines Gesetzgebungsaktes als wesentlich und welche als nicht wesentlich betrachtet werden können. Auch die europäische Rechtsprechung gibt hierauf keine eindeutige Antwort. In der Rechtsprechung des EuGH wird der Art. 290 AEUV so ausgelegt, dass der Erlass einer Regelung, die sich mit den wesentlichen Aspekten einer Materie befasst, „politische Entscheidungen“ benötigt, die „in die eigene Zuständigkeit des Unionsgesetzgebers fallen.“[21] Solche wesentlichen Aspekte sind somit der Entscheidung des Europäischen Parlaments und des Rates vorbehalten.

Im Rahmen einer interinstitutionellen Vereinbarung haben das Europäische Parlament, der Rat und die Kommission nicht bindende Kriterien für die Anwendung der Art. 290 AEUV erarbeitet[22]. Aus diesen geht hervor, dass zusätzliche Vorschriften, die auf dem Inhalt des Basisrechtsaktes aufbauen oder ihn weiterentwickeln, mittels delegierter Rechtsakte festgelegt werden können. Allerdings gibt es keine Erläuterungen dazu, inwiefern sich politische und damit wesentliche von technischen und damit nicht wesentlichen Entscheidungen unterscheiden. Letztlich muss daher im Einzelfall geprüft werden, ob ein scheinbar technischer Aspekt nach näherer Betrachtung eine politische Bedeutung haben könnte.

Als problematisch können hier die Vorschriften des CRA angesehen werden, nach denen die Kommission mittels delegierter Rechtsakte festlegen darf, welche Produkte mit digitalen Elementen als kritisch (Klassen I und II) sowie als hochkritisch eingestuft werden sollen [Art. 6 Abs. 2 S. 1, Abs. 3 und 5]. Mit dieser Befugnis erhält die Kommission das Recht den Anwendungsbereich des CRA genauer zu spezifizieren. Sie entscheidet damit im Kern auch darüber, welche PmdE einem strengeren und welche einem milderen Rechtsrahmen unterliegen. Denn insbesondere die Strenge der geforderten Konformitätsbewertungen steigt mit der eingestuften Kritikalität eines PmdE.

Ob die, auf den ersten Blick technisch anmutenden Ergänzungen oder Anpassungen der Einstufung von Kategorien von PmdE als kritisch, hochkritisch oder unkritisch tatsächlich komplett frei von politischen Erwägungen getroffen werden kann und wird, lässt sich zwar nicht eindeutig voraussehen, darf aber zumindest angezweifelt werden. Zwar schreibt der CRA Kriterien vor, die die Kommission als Grundlage für die Einstufung der Kritikalität einer Kategorie von PmdE heranziehen muss, sodass willkürliche und unbegründete Einstufungsentscheidungen ausgeschlossen werden können. Allerdings behält die Kommission einen gewissen Ermessungsraum bei den Einstufungen, da der CRA Vorschlag keine klaren und eindeutigen Vorgaben dazu enthält, wie die Abgrenzung von PmdE der Klassen I und II sowie zwischen kritischen und hochkritischen PmdE vorzunehmen ist. So nennt die Kommission etwa für die Einordnung in die Klassen I und II zwar 5 Kriterien, sie legt aber nicht fest, welche Kriterien zu welchem Grad erfüllt sein müssen, damit ein Produkt entweder in Klasse I oder II fällt. Außerdem muss die Kommission keine Argumentation zur Einstufung der PmdE in die Risikogruppen abgeben. Es wird deshalb auch nicht transparent, welche Kriterien sie, zu welchem Grad bei einer Einstufung heranziehen wird bzw. welchen sie Vorrang eingeräumt hat.

---

21 Urteil des Gerichtshofes (Große Kammer) vom 5. September 2012, Parlament/Rat, C-355/10, EU:C:2012:516, Rn. 65.

22 Nicht bindende Kriterien vom 18. Juni 2019 für die Anwendung der Artikel 290 und 291 des Vertrags über die Arbeitsweise der Europäischen Union (im Folgenden Nicht bindende Kriterien für die Anwendung der Artikel 290 und 291), 2019/C 223/01, ABl. C 223/1.

Letztlich ist daher durchaus denkbar, dass die Einstufung einer Kategorie von PmdE in eine bestimmte Risikogruppe in der Praxis keine rein technische Entscheidung darstellt, auch wenn sich die Kommission strikt an den im CRA vorgegebenen Kriterienkatalog hält. Dies gilt schon allein deshalb, weil der Einsatz eines bestimmten PmdE in einer sensiblen Umgebung, d.h. bspw. bei einem Betreiber einer kritischen Infrastruktur, wie die vergangenen Monate und Jahre gezeigt haben, hochpolitisch sein kann. Erinnert sei hier etwa an die fortdauernde Diskussion über den Einsatz von Technik des Telekommunikationsausrüsters Huawei, etwa beim 5G-Netzausbau. In solchen Fällen könnte es politisch geboten bzw. opportun sein, eine höhere Risikoeinstufung vorzunehmen und strengere Prüfmaßstäbe an die Cybersicherheit anzusetzen, obgleich diese aus rein technischer Perspektive ggfs. nicht in jedem Fall (zwingend) notwendig wäre. Sollte die Kommission daher die Befugnis erhalten, PmdE eigenständig in Risikogruppen einstufen zu dürfen, ist zu vermuten, dass solche Entscheidungen regelmäßig nicht nur rein technischer Natur sein werden, sondern auch politische Erwägungen eine Rolle spielen, darunter solche, die zusätzliche Markteintrittsbarriere schaffen, beispielsweise wenn die betroffenen PmdE im Großteil im Ausland hergestellt werden.

Trotz der oben dargelegten Problematiken, die mit dem Erlass delegierter Rechtsakte einhergehen könnten, hat die Delegierung der Befugnisse und die damit einhergehende Möglichkeit der Änderung des Gesetzgebungsaktes auch Vorteile. Rechtstechnisch sind delegierte Rechtsakte ein wirksames Instrument, das dazu beiträgt, die Gesetzgebung auf dem aktuellen Stand zu halten. Mit einer Rechtsnorm, die der Kommission das Recht zum Erlass eigener Rechtsakte delegiert, kann der Gesetzgeber das Verfahren zu Gesetzesanpassungen in benannten Bereichen bestimmen. Der Erlass eines delegierten Aktes ist eindeutig eine schnellere und einfachere Option als der Umweg über ein ordentliches Gesetzgebungsverfahren. Mittels delegierter Akte kann die Kommission rasch auf Marktänderungen und das Aufkommen neuer Technologien und PmdE reagieren. Sie ist zügig in der Lage neue kritische oder hochkritische PmdE zu identifizieren und die Listen für Kategorien kritischer bzw. hochkritischer Produkte zu aktualisieren.

D. Fazit

Die EU-Kommission hat mit dem CRA einen ambitionierten Rechtsrahmen zur Erhöhung der Cybersicherheit von Produkten mit digitalen Elementen vorgelegt und man muss der Kommission zu diesem gelungen Rechtsakt gratulieren. Denn der CRA leistet einen wesentlichen Beitrag zur Behebung von zahlreichen Defiziten, die den Märkten für diese Produkte innewohnen. So wird der CRA die Hersteller von PmdE dazu bewegen, mehr in die Cybersicherheit ihrer Produkte zu investieren und diesbezüglichen bestehenden Fehlanreizen entgegenwirken. Auch wird er potenzielle Käufer von PmdE befähigen, die Cybersicherheit der Produkte stärker in ihre Erwerbsentscheidung einbeziehen zu können. Einige der vorgeschlagenen Regelungen bedürfen jedoch noch eines Finetunings. So ist die von der Kommission vorgenommene Einstufung von Produkten in die Klassen 1 und 2 für kritische Produkte undurchsichtig und nicht schlüssig. Auch die Befugnisübertragung an die Kommission zum Erlass delegierter Rechtsakte über die Anpassung der Listen für (hoch)kritische Produkte ist aus juristischer Sicht nicht unproblematisch, da hier leicht politische Erwägungen bei den Kommissionsentscheidungen mit ins Spiel kommen könnten und nicht nur rein technische Überlegungen. Ferner ist die Kohärenz mit anderen EU-Rechtsakten teilweise noch nicht gegeben, wie etwa bei der Dauer der Pflicht zur Schwachstellenbehebung, die von kürzlich festgelegten Ökodesignvorgaben für Smartphones, Tablets und Mobiltelefonen abweichen. Zuletzt ist auch zu prüfen, ob der Geltungsbeginn des CRA von zwei Jahren nach Inkrafttreten des CRA nicht zu ambitioniert ist. Ungeachtet der Dringlichkeit zur Stärkung der Cybersicherheit in der EU, sollte den betroffenen Wirtschaftsakteure und auch den Aufsichtsbehörden hier mehr Zeit eingeräumt werden.

E. Anhänge

1 Anhang I: Produkte mit digitalen Elementen

Nicht-kritische PmdE (d.h. alle PmdE, die keine kritischen oder hochkritische PmdE sind), z.B.	Kritische PmdE (Klasse 1)	Kritische PmdE (Klasse 2)	Hochkritische PmdE
Intelligente Lautsprecher	Software für Identitätsverwaltungssysteme und Benutzerzugriffskontrollsoftware	Betriebssysteme für Server, Desktops und Mobilgeräte	Noch offen
Textverarbeitung	Eigenständige und eingebettete Browser	Hypervisoren und Container-Laufzeitsysteme mit visualisierten Betriebssystemen	
Fotobearbeitung	Passwort-Manager	Public-Key-Infrastruktur und Aussteller digitaler Zertifikate	
Computerspiele	Software, die bösartige Software sucht, entfernt oder absondert	Firewalls und Präventionssysteme für industrielle Nutzung	
Festplatten	Produkte mit digitalen Elementen mit der Funktion eines virtuellen privaten Netzwerks (VPN)	Mikroprozessoren für allgemeine Zwecke	
	Netzverwaltungssysteme	Mikroprozessoren zur Integration in speicherprogrammierbare Steuerungen und sichere Elemente	
	Tools zur Verwaltung der Netzwerkkonfiguration	Routers, Modems zur Verbindung mit Internet und Switches für industrielle Nutzung	
	Systeme zur Überwachung des Netzwerkverkehrs	Sicherungselemente	
	Verwaltung von Netzwerkressourcen	Hardware-Sicherheitsmodule (HSM)	
	SIEM-Systeme (Security Information und Event Management)	Sichere Kryptoprozessoren	
	Patch- oder Aktualisierungsmanagement	Smartcards, Smartcard-Lesegeräte und Token	
	Verwaltungssysteme für die Anwendungskonfiguration	Industrielle Automatisierungs- und Steuerungssysteme (IACS), die von kritischen Einrichtungen verwendet werden	
	Fernzugriffs-/Freigabesoftware	Geräte des industriellen Internets der Dinge, die von kritischen Einrichtungen verwendet werden	

	Software zur Verwaltung mobiler Geräte	Produkte zur Verleihung von Sensorfähigkeiten an Roboter, Aktoren und Robotersteuerungen	
	Physikalische Netzwerkschnittstellen	Intelligente Zähler	
	Betriebssysteme, die nicht unter Klasse II fallen		
	Firewalls, Angriffserkennungs- und/oder Angriffsverhinderungssysteme, die nicht unter Klasse II fallen		
	Router, Modems für Internetanschluss und Switches, die nicht unter Klasse II fallen		
	Mikroprozessoren, die nicht unter Klasse II fallen		
	Mikrocontroller		
	Anwendungsspezifische integrierte Schaltungen (ASIC) und feldprogrammierbare Gate-Arrays (FPGA), die von kritischen Einrichtungen verwendet werden		
	Industrielle Automatisierungs- und Steuerungssysteme (IACS), die nicht unter Klasse II fallen		
	Industrielles Internet der Dinge, das nicht unter Klasse II fällt		

2 Anhang II: Anzuwendende Konformitätsbewertungsverfahren

Konformitätsbewertungsverfahren basierend auf einer internen Kontrolle (Modul A)

Der Hersteller muss

- sicherstellen und auf eigene Verantwortung erklären, dass das PmdE alle grundlegenden Cybersicherheitsanforderungen entspricht,
- eine technische Dokumentation erstellen,
- alle erforderlichen Maßnahmen treffen, damit die Verfahren der Konzeption, Entwicklung, Herstellung und Schwachstellenbehandlung und deren Überwachung mit den grundlegenden Cybersicherheitsanforderungen konform sind,
- das CE-Konformitätskennzeichen auf jedem konformen PmdE anbringen,
- für jedes PmdE eine Konformitätserklärung ausstellen und sie für zehn Jahre ab dem Inverkehrbringen des Produkts aufbewahren.

EU-Baumusterprüfung (Modul B)

Bei der EU-Baumusterprüfung prüft und attestiert eine benannte Stelle die technische Konzeption und Entwicklung des PmdE und die vom Hersteller eingerichteten Verfahren zum Umgang mit Schwachstellen.

Die Hersteller dürfen eine benannte Stelle ihrer Wahl beauftragen. Diese prüft die technische Dokumentation und zusätzlich eingereichte Nachweise sowie die Muster von einem oder mehrerer wichtiger Teile des Produkts (Kombination aus Bau- und Konzeptionsmuster), insbesondere auch ob Produkte bzw. Muster und eingerichtete Prozesse den harmonisierten Normen und/oder technischen Spezifikationen entsprechen.

Die benannte Stelle verfasst einen Bewertungsbericht, in dem sie die Ergebnisse der durchgeführten Untersuchungen darlegt. Die Veröffentlichung des Berichts bedarf der Zustimmung des Herstellers.

Entsprechen Baumuster und die Verfahren zur Behandlung von Schwachstellen den Anforderungen, kann die die benannte Stelle dem Hersteller eine EU-Baumusterprüfbescheinigung ausstellen. Die Bescheinigung muss alle relevanten Informationen enthalten, die die Konformität nachweisen.

Die Hersteller müssen die benannte Stelle über alle Änderungen am zugelassenen Baumuster und Verfahren zur Behandlung von Schwachstellen informieren. Solche Änderungen bedürfen einer zusätzlichen Genehmigung in Form einer Ergänzung der ursprünglichen EU-Baumusterprüfbescheinigung.

Konformität mit dem Baumuster basierend auf interner Fertigungskontrolle (Modul C)

Bei diesem Konformitätsbewertungsverfahren muss der Hersteller alle erforderlichen Maßnahmen treffen, damit das hergestellte PmdE mit dem in der EU-Baumusterprüfbescheinigung beschriebenen zugelassenen Baumuster konform ist sowie den grundlegenden Cybersicherheitsanforderungen genügt.

Der Hersteller muss zudem an jedem PmdE, das mit dem in der EU-Baumusterprüfbescheinigung beschriebenen Baumuster übereinstimmt und die Cybersicherheitsanforderungen erfüllt, das CE-Kennzeichen anbringen. Zudem muss er eine Konformitätserklärung für jedes PmdE-Produktmodell ausstellen und für zehn Jahre nach dem Inverkehrbringen aufbewahren.

Konformitätsbewertungsverfahren basierend auf vollständiger Qualitätssicherung (Modul H)

Bei diesem Konformitätsbewertungsverfahren erklärt der Hersteller eigenverantwortlich, dass sein PmdE und die Verfahren zum Umgang mit Schwachstellen mit den Anforderungen konform sind.

Die Hersteller müssen für die Konzeption, Entwicklung und Herstellung des PmdE und für die Behandlung von Schwachstellen ein zugelassenes Qualitätssicherungssystem betreiben und dessen Wirksamkeit während des gesamten Lebenszyklus des betreffenden Produkts aufrechterhalten. Das Qualitätssicherungssystem muss durch eine benannte Stelle überprüft und genehmigt werden.

Die Hersteller müssen die benannte Stelle über jede beabsichtigte Änderung des Qualitätssicherungssystems informieren. Die Stelle prüft die Änderungen und muss entscheiden, ob eine Neubewertung notwendig ist.

Die Hersteller müssen sicherstellen, dass die benannten Stellen prüfen können, ob sie die mit dem zugelassenen Qualitätssicherungssystem verbundenen Pflichten vorschriftsmäßig erfüllen. Die Stellen führen hierfür auch regelmäßige Audits durch.

Die Hersteller müssen an jedem PmdE, das den Anforderungen genügt, das CE-Kennzeichen anbringen. Zudem muss er eine Konformitätserklärung für jedes PmdE-Produktmodell ausstellen und für zehn Jahre nach dem Inverkehrbringen aufbewahren.