Der Entwurf des Cyber Resilience Act

I. Einleitung

Am 15.9.2022 hat die EU-Kommission den lange erwarteten Entwurf der „Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020" (kurz: „Cyber Resilience Act" oder CRA-E) vorgelegt. Die Reichweite der neu eingeführten Pflichten für Hersteller, Händler und Importeure von Produkten mit digitalen Elementen wie auch die Risiken im Falle der Nichteinhaltung dieser sind enorm. Um das Risiko hoher Kosten im Rahmen der kurzfristigen oder nachträglichen Anpassung von Geschäftsabläufen oder Produktionsprozessen zu vermeiden, wird die frühzeitige Verfolgung der weiteren Entwicklungen dringend empfohlen.

II. Hintergrund

Hard- und Software-Produkte sind zunehmend Gegenstand erfolgreicher Cyberangriffe. Bis einschließlich 2021 führte dieser Umstand zu geschätzten jährlichen Kosten in Höhe von 5,5 Billionen EUR weltweit.[1] Viele Hard- und Software-Produkte leiden unter zwei großen Problemen, die den Nutzern und der Gesellschaft zusätzliche Kosten verursachen: einem niedrigen Cyber-Sicherheitsniveau, das sich in teils weit verbreiteten Schwachstellen und der unzureichenden und uneinheitlichen Bereitstellung von Sicherheitsupdates zu deren Behebung widerspiegelt, und einem unzureichenden Verständnis

1 Explanatory Memorandum CRA-E, S. 1.

und unzureichendem Zugang zu Informationen aufseiten der Nutzer, was sie daran hindert, solche Produkte auszuwählen, die über angemessene Cyber-Sicherheitseigenschaften verfügen, bzw. diese auf eine Weise zu nutzen, die den Cyber-Sicherheitsrisiken gerecht wird. Dies ist insbesondere deshalb problematisch, weil in einer vernetzten Welt ein Cyber-Sicherheitsvorfall bei einem Produkt ein ganzes Unternehmen oder eine ganze Lieferkette in Mitleidenschaft ziehen und sich oft innerhalb weniger Minuten über ein gesamtes Ökosystem hinweg ausbreiten kann. Dies kann zu einer schwerwiegenden Unterbrechung wirtschaftlicher und sozialer Aktivitäten führen oder sogar lebensbedrohlich werden.

Der bestehende EU-Rechtsrahmen gilt zwar für bestimmte solcher Produkte, doch für die meisten gibt es derzeit keine EU-Vorschriften, die Mindestanforderungen an die Cyber-Sicherheit der Produkte festlegen. Dies gilt insbesondere für die Cyber-Sicherheit von sog. Non-embedded-Software, also zB Betriebssystemen von Endgeräten wie Windows, macOS oder die verschiedenen Linux Distributionen, auch wenn Cyberangriffe zunehmend auf Schwachstellen in genau diesen Produkten abzielen. Es gibt zahlreiche Beispiele für erfolgreiche Cyber-, insbesondere Ransomware-Angriffe, die auf unzureichende Cyber-Sicherheit der Produkte zurückzuführen sind. Hierzu zählen etwa die Angriffsserien „WannaCry“[2] und „NotPetya“[3] oder der Angriff auf die Lieferkette von Kaseya VSA durch die Hacker-Gruppe REvil.[4]

Vor diesem Hintergrund hat die EU Kommission zwei Hauptziele festgelegt, die die Funktionsfähigkeit des EU-Binnenmarktes sicherstellen sollen:[5] Schaffung von Bedingungen für die Entwicklung sicherer Produkte mit digitalen Elementen, indem sichergestellt wird, dass Hard- und Software-Produkte mit weniger Schwachstellen auf den Markt gebracht werden, und die Hersteller die Sicherheit während des gesamten Lebenszyklus eines Produkts ernstnehmen, und Schaffung von Bedingungen, die es den Nutzern ermöglichen, die Cyber-Sicherheit bei der Auswahl und Verwendung von Produkten mit digitalen Elementen zu berücksichtigen. Zur Erreichung dieser Hauptziele wurden vier Ziele formuliert, die Grundlage des CRA-E sind: (1) Gewährleistung, dass die Hersteller die Sicherheit von Produkten mit digitalen Elementen von der Entwurfs- und Entwicklungsphase an und während des gesamten Lebenszyklus verbessern; (2) Gewährleistung eines kohärenten Cyber-Sicherheitsrahmens, der die Einhaltung der Vorschriften für Hard- und Softwarehersteller erleichtert; (3) Verbesserung der Transparenz der Cyber-Sicherheitseigenschaften von Produkten mit digitalen Elementen und (4) Befähigung von Unternehmen und Verbrauchern, Produkte mit digitalen Elementen sicher zu nutzen.

III. Der Entwurf des Cyber Resilience Act

1. Anwendungsbereich

Das einschlägige Unionsrecht umfasst mehrere horizontale Rechtsakte, die verschiedene Aspekte im Zusammenhang mit Cyber-Sicherheit aus unterschiedlichen Blickwinkeln behandeln, einschließlich Maßnahmen zur Verbesserung der Sicherheit digitaler Lieferketten. Da diese Rechtsakte jedoch nur sektoral und damit nur für bestimmte Produkte mit digitalen Elementen gelten, gibt es bislang keinen Rechtsakt im Unionsrecht, der allgemeine, sektorübergreifende Anforderungen an die Cyber-Sicherheit aller Produkte mit digitalen Elementen festlegt. So enthalten beispielsweise die Verordnungen (EU) 2017/745[6] und (EU) 2017/746[7] Vorschriften für Medizinprodukte und In-vitro-Diagnostika. Art. 4 Abs. 5 lit. d) der VO (EU) 2019/2144 legt Anforderungen für die Typgenehmigung von Fahrzeugen und ihren Systemen und Bauteilen fest und führt Cyber-Sicherheitsanforderungen ein, unter anderem für den Betrieb eines zertifizierten Cyber-Sicherheits-Managementsystems, für Software-Updates, für Organisationsstrategien und -verfahren für Cyberrisiken im Zusammenhang mit dem gesamten Lebenszyklus von Fahrzeugen, Ausrüstungen und Diensten im Einklang mit den geltenden Vorschriften der Vereinten Nationen über technische Spezifikationen und Cyber-Sicherheit sowie für spezifische Konformitätsbewertungsverfahren.

2. Produkte mit digitalen Elementen

Nach Art. 3 Nr. 1 CRA-E ist ein Produkt mit digitalen Elementen „jedes Soft- oder Hardware-Produkt und seine Ferndatenverarbeitungslösungen, einschließlich Software- oder Hardware-Komponenten, die separat in Verkehr gebracht werden sollen“. Ferndatenverarbeitung ist nach Art. 3 Nr. 2 des Entwurfs des Cyber Resilience Act dabei „jede Datenverarbeitung aus der Ferne, für die die Software vom Hersteller oder unter der Verantwortung des Herstellers konzipiert und entwickelt wurde und deren Fehlen das Produkt mit digitalen Elementen daran hindern würde, eine seiner Funktionen zu erfüllen“.

a) Kritische und hochkritische Produkte mit digitalen Elementen

Neben „normalen“ Produkten mit digitalen Elementen umfasst der Entwurf des Cyber Resilience Act auch „kritische“ Produkte mit digitalen Elementen. Innerhalb der „kritischen“ Produkte mit digitalen Elementen wird zwischen „kritischen“ und „hochkritischen“ Produkten unterschieden. Ob ein Produkt ein solches „kritisches“ bzw. „hochkritisches“ Produkt mit digitalen Elementen darstellt, richtet sich danach, ob die Kernfunktion dieses Produkts einer der in Annex III zum CRA-E aufgelisteten Kategorien entspricht, und wie hoch das Cyber-Sicherheitsrisiko ist, welches vom jeweiligen Produkt ausgeht. Bei der Ermittlung des Cyber-Sicherheitsrisikos sind die in Art. 6 Abs. 2 CRA-E aufgeführten Kriterien zu berücksichtigen.

„Kritische“ und „hochkritische“ Produkte mit digitalen Elementen werden in Annex III zum CRA-E genauer beschrieben. Zu kritischen Produkten, Klasse I in Annex III zum CRA-E, gehören etwa Identitätsmanagementsysteme, Browser,

2 Bundesamt für Sicherheit in der Informationstechnik, Ransomware – Vorsicht vor Erpressersoftware, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Schadprogramme/Ransomware/ransomware_node.html.
3 Ebenda.
4 BSI-Report zur Lage der IT-Sicherheit in Deutschland 2022, S. 36.
5 Siehe Explanatory Memorandum CRA-E, S. 1.
6 Pflichtenkatalog für Hersteller für das Inverkehrbringen medizinischer Produkte, Art. 10 ff. VO (EU) 2017/745.
7 Pflichtenkatalog für Hersteller für das Inverkehrbringen von In-vitro-Diagnostika, Art. 10 ff. VO (EU) 2017/746.

Passwortmanager, Antivirenprogramme, Firewalls, virtuelle private Netzwerke (VPNs), Netzwerkmanagement-Systeme, physische Netzwerkschnittstellen, Router, Chips, die für wesentliche Einrichtungen im Sinne der kürzlich überarbeiteten Richtlinie zur Netz- und Informationssicherheit NIS 2 verwendet werden, und alle Betriebssysteme, Mikroprozessoren und das industrielle IoT, die nicht unter Klasse II fallen.

Hochkritische Produkte umfassen, nach Klasse II, etwa Betriebssysteme für Server, Desktops und Mobilgeräte, in Hypervisors und Containern virtualisierte Betriebssysteme, Aussteller digitaler Zertifikate, Allzweck-Mikroprozessoren, Kartenlesegeräte, Robotersensoren, intelligente Messgeräte und alle IoT-Geräte, Router und Firewalls für den industriellen Einsatz, der als „sensible Umgebung" gilt.

Sowohl die Liste der Klasse I-, als auch die der Klasse II-Produkte ist nicht abschließend. Um die Listen dieser Produkte zu aktualisieren oder anzupassen und daneben auch weitere Vorgaben zur Zertifizierung von hochkritischen Produkten aufzunehmen, sollen der EU-Kommission nach Art. 6 Abs. 5 CRA-E umfangreiche Rechte zur Anpassung des Entwurfs des Cyber Resilience Act eingeräumt werden.

Die Einordnung eines Produkts mit digitalen Elementen als kritisches oder hochkritisches Produkt mit digitalen Elementen und auch die Einordnung innerhalb der kritischen Produkte in Klasse I oder Klasse II haben erheblichen Einfluss auf die Anforderungen, die der Entwurf des Cyber Resilience Act an die Produktkonformität stellt.

b) Hochrisiko-KI-Systeme

Eine weitere Produktgruppe im Entwurf des Cyber Resilience Act stellen nach Art. 8 CRA-E sog. „Hochrisiko-KI-Systeme" dar. Hierbei soll sich sowohl die Einordnung als ein solches Hochrisiko-KI-System, als auch die Konformitätsprüfung primär nach den Anforderungen der KI-Verordnung richten, welche zum aktuellen Zeitpunkt noch ausschließlich als Entwurf vorliegt. Sofern ein Produkt mit digitalen Elementen die Konformitätsanforderungen der KI-Verordnung erfüllt, sollen die entsprechenden Voraussetzungen des CRA-E ebenfalls als erfüllt gelten. Ausgenommen von dieser Fiktion sind nach Art. 8 Abs. 3 CRA-E solche Hochrisiko KI-Systeme, für die die Durchführung einer Konformitätsprüfung nach den Art. 24 Abs. 2 lit. a, b, Abs. 3 lit. a, b CRA-E vorgeschrieben ist, und die im Rahmen der KI-Verordnung eine Konformitätsprüfung auf Grundlage interner Überprüfungen durchführen konnten.

c) Bereichsausnahmen

aa) Open Source Software

Besonderes Augenmerk wird nach dem Entwurf des Cyber Resilience Act auf Open Source Software (OSS) zu richten sein. Nach Erwägungsgrund 10 des Entwurfs des Cyber Resilience Act soll OSS generell aus dem Anwendungsbereich der Verordnung ausgenommen werden. Frei übersetzt beschreibt der Erwägungsgrund:

„Um Innovation und Forschung nicht zu behindern, sollte freie und quelloffene Software, die außerhalb einer gewerblichen Tätigkeit entwickelt oder bereitgestellt wird, nicht unter diese Verordnung fallen. Dies gilt insbesondere für Software, einschließlich ihres Quellcodes und geänderter Versionen, die offen gemeinsam genutzt wird und frei zugänglich, nutzbar, veränderbar und weiterverteilbar ist."

Wie weit diese Ausnahme reichen soll, bleibt zu klären. Der Umfang dieser Ausnahme ist allerdings insofern von Bedeutung, als im Rahmen des Einsatzes von OSS, neben ihrer Verwendung als „abtrennbarer" Teil eines Software-Produkts, auch die Möglichkeit besteht, sie so in ein Software-Produkt einzubinden, dass die OSS ein untrennbarer Teil des Produkts wird. Ob auch die auf diese Weise in einem Produkt mit digitalen Elementen eingebundene OSS vom Anwendungsbereich der Verordnung ausgenommen sein soll, kann dem Wortlaut des Erwägungsgrundes nicht abschließend entnommen werden. Der Wortlaut ließe sich vielmehr sowohl so auslegen, dass OSS generell einer Bereichsausnahme unterliegt, als auch so, dass nur die außerhalb einer gewerblichen Tätigkeit entwickelte oder bereitgestellte OSS als solche, nicht aber die in ein Produkt mit digitalen Elementen untrennbar eingebundene OSS, in die Bereichsausnahme fällt.

Wie allerdings ein Hersteller, der OSS als untrennbaren Teil in ein Produkt mit digitalen Elementen einbindet, die Verpflichtungen des Entwurfs des Cyber Resilience Act vollumfänglich erfüllen können soll, bleibt zu klären.

bb) Sektorspezifische Cyber-Sicherheitsanforderungen

Um die Regelung der eingangs erwähnten sektoralen Besonderheiten nicht durch den Entwurf des Cyber Resilience Act zu konterkarieren, soll der Cyber Resilience Act zwar nach Art. 2 Abs. 1 CRA-E grundsätzlich für alle Produkte mit digitalen Elementen gelten, „deren bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung zu einem Gerät oder Netz hat". Ausgenommen hiervon sind jedoch all solche Produkte mit digitalen Elementen, die gemäß Art. 2 Abs. 2 CRA-E Gegenstand einer der vorgenannten Verordnungen sind, gemäß Art. 2 Abs. 3 CRA-E nach der Verordnung 2018/1139 zertifiziert wurden oder gemäß Art. 2 Abs. 5 CRA-E ausschließlich der nationalen Sicherheit oder militärischen Zwecken dienen bzw. ausschließlich für die Verarbeitung geheimhaltungsbedürftiger Informationen entwickelt wurden.

3. Normadressaten des Entwurfs des Cyber Resilience Act

Hinsichtlich des Adressatenkreises richtet sich der Entwurf des Cyber Resilience Act, wie dies bereits aus anderen Bereichen des Produktsicherheitsrechts bekannt ist, an Hersteller, Importeure und Händler.

Hierbei ist Hersteller gem. Art. 3 Nr. 18 CRA-E „jede natürliche oder juristische Person, die Produkte mit digitalen Elementen entwickelt oder herstellt oder Produkte mit digitalen Elementen entwerfen, entwickeln oder herstellen lässt und sie unter ihrem Namen oder ihrer Marke vermarktet, unabhängig davon, ob dies entgeltlich oder unentgeltlich geschieht". Dieses, im europäischen Produktsicherheitsrecht verbreitete, weite Begriffsverständnis erfasst neben dem Hersteller klassischer „Eigenproduktionen" etwa auch natürliche oder juristi-

sche Personen, die Software-Produkte durch Dritte herstellen lassen oder White-Label-Lösungen anpassen und anschließend als Hersteller vertreiben.[8]

Unter den Begriff des Importeurs fällt nach Art. 3 Nr. 20 CRA-E „jede in der Union ansässige natürliche oder juristische Person, die ein Produkt mit digitalen Elementen, das den Namen oder die Marke einer außerhalb der Union ansässigen natürlichen oder juristischen Person trägt, in Verkehr bringt".

Händler ist demgegenüber nach Art. 3 Nr. 21 CRA-E „jede natürliche oder juristische Person in der Lieferkette, die nicht der Hersteller oder Importeur ist, die ein Produkt mit digitalen Elementen auf dem Unionsmarkt bereitstellt, auf dem Unionsmarkt verfügbar macht, ohne seine Eigenschaften zu beeinträchtigen".

Importeure oder Händler gelten als Hersteller, wenn sie nach Art. 15 CRA-E das Produkt mit digitalen Elementen im eigenen Namen in Verkehr bringen oder ein bereits in Verkehr gebrachtes Produkt mit digitalen Elementen substantiell verändern. Führt ein Dritter derartige Veränderungen am Produkt mit digitalen Elementen durch, gilt auch dieser nach Art. 16 CRA-E als Hersteller.

Hersteller, Importeure und Händler haben entwickelte oder zu vertreibende Produkte an den Vorgaben des Entwurfs des Cyber Resilience Act zu messen, wenn, im Falle von Herstellern und Importeuren, sie die Produkte mit digitalen Elementen „in Verkehr bringen", bzw., im Falle von Händlern, sie die Produkte mit digitalen Elementen „auf dem Markt bereitstellen".

„Inverkehrbringen" (engl. placing on the market) ist hierbei gemäß Art. 3 Nr. 22 CRA-E „die erstmalige Bereitstellung eines Produkts mit digitalen Elementen auf dem EU-Binnenmarkt". Ein Inverkehrbringen kann daher ausschließlich durch Händler und Importeure erfolgen.[9] Inverkehrbringen liegt hierbei immer dann vor, wenn ein Produkt zum ersten Mal an einen Händler oder einen Endverbraucher geliefert wird. Jeder nachfolgende Vorgang, zB von einem Händler an einen Händler oder von einem Händler an einen Endverbraucher, stellt eine „Bereitstellung auf dem Markt" dar.[10]

„Bereitstellen auf dem Markt" (engl. making available on the market) ist demgegenüber gem. Art. 3 Nr. 23 CRA-E „jede Bereitstellung eines Produkts mit digitalen Elementen zum Vertrieb oder zur Nutzung auf dem EU-Binnenmarkt im Rahmen einer gewerblichen Tätigkeit entgeltlich oder unentgeltlich". Dies umfasst jedes Angebot zum Vertrieb, Verbrauch oder zur Verwendung auf dem Unionsmarkt, das zu einer tatsächlichen Lieferung führen könnte (zB eine Aufforderung zum Kauf, Werbekampagnen).[11] Die Lieferung eines Produkts gilt allerdings nur dann als Bereitstellung auf dem Unionsmarkt, wenn das Produkt für die Endnutzung auf dem Unionsmarkt bestimmt ist.[12] Die Lieferung von Produkten für den weiteren Vertrieb, für die Verwendung in einem Endprodukt oder für die weitere Verarbeitung oder Veredelung mit dem Ziel, das Endprodukt außerhalb des Unionsmarktes auszuführen, gilt daher nicht als Bereitstellen auf dem Markt.

Sowohl der Begriff des „Inverkehrbringens", als auch der des „Bereitstellens auf dem Markt" bezieht sich auf jedes einzelne Produkt mit digitalen Elementen, nicht auf einen Produkttyp, und darauf, ob es als Einzelstück oder in Serie hergestellt wurde. Auch wenn ein Produktmodell oder -typ vor dem Inkrafttreten neuer Harmonisierungsrechtsvorschriften der EU, die neue verbindliche Anforderungen festlegen, geliefert wurde, müssen daher einzelne Einheiten desselben Modells oder Typs, die nach dem Inkrafttreten der neuen Anforderungen in Verkehr gebracht werden, diesen neuen Anforderungen entsprechen.

4. Pflichten der Wirtschaftsakteure

Art. 5 CRA-E beschreibt die allgemeine Verpflichtung, Produkte mit digitalen Elementen nur dann auf dem Markt bereitzustellen, wenn sie erstens die in Anhang I Abschnitt 1 zum Entwurf des Cyber Resilience Act genannten grundlegenden Sicherheitsanforderungen erfüllen, sofern sie ordnungsgemäß installiert, gewartet, bestimmungsgemäß oder unter vernünftigerweise vorhersehbaren Bedingungen verwendet und gegebenenfalls aktualisiert werden, und zweitens die vom Hersteller eingerichteten Verfahren den grundlegenden Anforderungen in Anhang I Abschnitt 2 zum Entwurf des Cyber Resilience Act entsprechen. Diese allgemeine Verpflichtung wird in den Art. 10 ff. CRA-E konkretisiert.

a) Die zentralen Pflichten der Hersteller

Der Entwurf des Cyber Resilience Act enthält eine umfangreiche Liste an Verpflichtungen, welche Hersteller von Produkten mit digitalen Elementen von der Planung bis zum Ende des Lebenszyklus des Produkts beachten müssen. Diese Pflichten lassen sich grob in Prozess- und Dokumentationspflichten (Art. 10 CRA-E) und Informations- und Meldepflichten (Art. 11 CRA-E) unterteilen.

aa) Prozess- und Dokumentationspflichten

Nach Art. 10 Abs. 1 CRA-E trifft die Hersteller zunächst die Verpflichtung, sicherzustellen, dass Produkte mit digitalen Elementen in Übereinstimmung mit den dem Entwurf des Cyber Resilience Act in Ziff. 1 der Anlage 1 angehängten grundlegenden Sicherheitsanforderungen (essential security requirements) entworfen, entwickelt und eingeführt werden.

Die Liste der grundlegenden Sicherheitsanforderungen umfasst (1) ein „angemessenes" Cyber-Sicherheitsniveau, (2) das Verbot, Produkte mit bekannten Schwachstellen auf den Markt zu bringen, (3) Sicherheit durch Standardkonfiguration, (4) Schutz vor unbefugtem Zugriff, (5) Begrenzung der Angriffsflächen und (6) Minimierung der Auswirkungen von Vorfällen.

Die Produkte mit digitalen Elementen müssen die Vertraulichkeit der Daten gewährleisten, ua durch Verschlüsselung, Schutz der Datenintegrität und Verarbeitung nur der Daten,

8 Albrecht GWR 2022, 313.
9 Bekanntmachung der Kommission – Leitfaden für die Umsetzung der Produktvorschriften der EU 2016 („Blue Guide"), S. 18.
10 Blue Guide S. 18.
11 Blue Guide S. 17.
12 Blue Guide S. 17.

die für das Funktionieren des Produkts unbedingt erforderlich sind.

Um der Verpflichtung aus Art. 10 Abs. 1 CRA-E nachzukommen, sollen die Hersteller nach Art. 10 Abs. 2 CRA-E eine Bewertung der mit einem Produkt mit digitalen Elementen verbundenen Cyber-Sicherheitsrisiken vornehmen und das Ergebnis dieser Bewertung in der Planungs-, Entwurfs-, Entwicklungs-, Produktions-, Liefer- und Wartungsphase des Produkts mit digitalen Elementen berücksichtigen, um die Cyber-Sicherheitsrisiken zu minimieren, Sicherheitsvorfälle zu verhindern und die Auswirkungen solcher Vorfälle, auch in Bezug auf die Gesundheit und Sicherheit der Nutzer, zu minimieren. Diese Bewertung der Cyber-Sicherheitsrisiken soll bei Inverkehrbringen von Produkten mit digitalen Elementen nach Art. 10 Abs. 3 CRA-E Teil der technischen Dokumentation gem. Art. 23 CRA-E sein, nach Art. 10 Abs. 5 CRA-E dokumentiert und in einer Weise, die der Art und Schwere der Cyber-Sicherheitsrisiken angemessen ist, regelmäßig aktualisiert werden. Nach Art. 10 Abs. 6 CRA-E müssen Hersteller darüber hinaus Schwachstellen während des gesamten Lebenszyklus des Geräts, höchstens allerdings für fünf Jahre durch automatische und kostenlose Updates überwachen und beheben. Art. 10 Abs. 7 CRA-E verpflichtet die Hersteller, vor dem Inverkehrbringen eines Produktes mit digitalen Elementen, zur Erstellung der in Art. 23 genannten technischen Dokumentation sowie zur Durchführung der gewählten Konformitätsbewertungsverfahren gem. Art. 24 CRA-E. Die Unterlagen zur technischen Dokumentation sowie die EU-Konformitätserklärung müssen nach dem Inverkehrbringen gemäß Art. 10 Abs. 8 CRA-E 10 Jahre lang vom Hersteller aufbewahrt werden. Die EU-Konformitätserklärung ist nach Art. 10 Abs. 11 CRA-E entweder dem Produkt mit digitalen Elementen beizufügen oder muss über einen Link in der technischen Dokumentation abrufbar sein,

Hersteller sind nach Art. 10 Abs. 9 CRA-E verpflichtet, Verfahren zur Einhaltung der Konformität bei Produkten mit digitalen Elementen, die Teil einer Produktionsreihe sind, einzuführen und aufrechtzuerhalten. Sie müssen sicherstellen, dass den Produkten mit digitalen Elementen die in Annex II genannten Informationen und Anleitungen in elektronischer und physischer Form in verständlicher Sprache beigefügt sind, Art. 10 Abs. 10 CRA-E.

Erlangt ein Hersteller nach Inverkehrbringen Kenntnis davon, oder hat er Gründe zur Annahme, dass das Produkt mit digitalen Elementen nicht den in Annex I aufgeführten grundlegenden Anforderungen entspricht, hat er gem. Art. 10 Abs. 12 CRA-E unverzüglich die erforderlichen Korrekturmaßnahmen zur Wiederherstellung der Konformität vorzunehmen bzw. das Produkt zurückzunehmen oder zurückzurufen. Diese Verpflichtung besteht während der voraussichtlichen Lebensdauer des Produkts, maximal jedoch für einen Zeitraum von fünf Jahren ab Inverkehrbringen.

bb) Informations- und Meldepflichten

Um all dies dauerhaft gewährleisten zu können, sollen die Hersteller verpflichtet werden, die Schwachstellen im Produkt durch regelmäßige Tests zu ermitteln und sie unverzüglich beheben.

Ähnlich wie die kürzlich überarbeitete Richtlinie zur Netz- und Informationssicherheit (NIS-2) enthält Art. 11 Abs. 1, 2 CRA-E eine Verpflichtung, ausgenutzte Schwachstellen und Zwischenfälle zu melden. Diese Meldung hat unverzüglich, spätestens aber innerhalb von 24 Stunden, nach Bekanntwerden einer aktiv ausgenutzten Sicherheitsschwachstelle oder nach Bekanntwerden von Zwischenfällen, welche Auswirkungen auf die Sicherheit der Produkte mit digitalen Elementen haben können, diese an die European Union Agency for Cybersecurity („ENISA“) zu melden. Zusätzlich enthält Art. 11 Abs. 4 CRA-E eine Verpflichtung des Herstellers, die Nutzer des Produkts mit digitalen Elementen über den Zwischenfall und, soweit erforderlich, Abhilfemaßnahmen zu informieren. Setzt der Hersteller in dem Produkt mit digitalen Elementen OSS ein, soll er nach Art. 11 Abs. 7 CRA-E zusätzlich verpflichtet sein, im Falle der Feststellung von Schwachstellen in der OSS den Betreiber der OSS über die Schwachstelle zu informieren.

Diese Erweiterung der Informations- und Meldepflichten kann im Falle eines Sicherheitsvorfalls durchaus eine gewisse Komplexität nach sich ziehen. Denn regelmäßig sind in diesen Fällen zeitgleich auch Meldungen zB an eine oder mehrere Datenschutzaufsichtsbehörden durchzuführen. Im Falle von Betreibern „wesentlicher oder wichtiger Einrichtungen“ im Sinne der NIS-2 können darüber hinaus Meldungen an die zuständigen nationalen Behörden oder die CSIRT erforderlich werden. Es empfiehlt sich daher, einen Prozess zur Durchführung aller relevanten Meldungen innerhalb der jeweils vorgesehenen Fristen zu etablieren.

b) Ernennung eines Bevollmächtigten

Nach Art. 12 CRA-E kann ein Hersteller einen Bevollmächtigten (engl. authorized representative) ernennen und an diesen einzelne Aufgaben, die nach dem Entwurf des Cyber Resilience Act dem Hersteller obliegen, delegieren. Gegenstand der Übertragung können nach Art. 12 Abs. 3 CRA-E insbesondere die Zusammenarbeit mit Marktüberwachungsbehörden, die Beantwortung von Anfragen dieser und die Aufbewahrung der technischen Dokumentation und der EU-Konformitätserklärung sein. Explizit ausgenommen sind nach Art. 12 Abs. 1 dagegen die Verpflichtungen nach Art. 10 Abs. 1 bis Abs. 7 UAbs. 1 und Abs. 9 CRA-E.

c) Pflichten der Importeure

Wie bereits aus anderen Bereichen des Produktsicherheitsrechts bekannt, wird im Rahmen des Entwurfs des Cyber Resilience Act nun auch Importeuren hinsichtlich der Cyber-Sicherheit von Produkten ein umfangreiches Paket an Pflichten auferlegt. Wie die Hersteller sind nach Art. 13 Abs. 1 CRA-E auch die Importeure von Produkten mit digitalen Elementen nach dem Entwurf des Cyber Resilience Act verpflichtet sicherzustellen, dass nur solche Produkte mit digitalen Elementen in Verkehr gebracht werden, die den grundlegenden Anforderungen (engl. essential requirements) aus Ziff. 1 des Annex I genügen, und für die der Hersteller Prozesse zum Umgang mit Schwachstellen eingeführt hat, die den Anforderungen der Ziff. 2 des Annex I entsprechen. Vor dem Inverkehrbringen hat der Importeur sicherzustellen, dass

- die geeigneten Konformitätsbewertungsverfahren vom Hersteller durchgeführt worden sind;
- der Hersteller die technische Dokumentation erstellt hat;
- das Produkt mit digitalen Elementen die CE-Kennzeichnung trägt und diesem die erforderlichen Informationen und die Gebrauchsanweisung beigefügt sind.

Zusätzlich haben Importeure nach Art. 13 Abs. 4 CRA-E ihren Namen bzw. ihre Firma und ihre Kontaktinformationen auf dem Produkt mit digitalen Elementen oder, falls dies nicht möglich ist, auf der Verpackung anzubringen. Hierbei ist allerdings zu beachten, dass ein Importeur, der ein Produkt im eigenen Namen auf den Markt bringt, nach dem Entwurf des Cyber Resilience Acts selbst als Hersteller des Produkts anzusehen ist, so dass die angebrachten Informationen eindeutig auf den Importeur bezogen sein sollten.

Daneben haben Importeure nach Art. 13 Abs. 5 CRA-E sicherzustellen, dass die Anleitungen und Informationen nach Annex II zum CRA-E dem Produkt beigefügt sind, und dies in einer Sprache, die von den Nutzern leicht verstanden werden kann.

Ebenso wie Hersteller sind Importeure nach Art. 13 Abs. 6 CRA-E verpflichtet, im Falle der Kenntniserlangung oder begründeten Annahme, dass ein von ihnen in Verkehr gebrachtes Produkt mit digitalen Elementen oder ein Prozess des Herstellers nach Annex I nicht konform zu den grundlegenden Anforderungen ist, unverzüglich Abhilfemaßnahmen zu ergreifen. Stellen Importeure Sicherheitsschwachstellen fest, sollen sie zusätzlich unverzüglich den Hersteller hierüber informieren. Folgt aus der Sicherheitsschwachstelle ein hohes Risiko für die Cybersecurity, besteht nach dem Entwurf des Cyber Resilience Act zusätzlich eine Informationspflicht der nationalen Marktüberwachungsbehörden der Mitgliedstaaten, in denen sie das Produkt mit digitalen Elementen in Verkehr gebracht haben.

Des Weiteren sind Importeure verpflichtet, die Konformitätserklärung für einen Zeitraum von 10 Jahren ab Inverkehrbringen aufzubewahren und sicherzustellen, dass die technische Dokumentation, zugehörig zum jeweiligen Produkt mit digitalen Elementen, auf Anfrage einer Marktüberwachungsbehörde bereitgestellt werden kann.

d) Pflichten der Händler

Händler von Produkten mit digitalen Elementen haben vor dem Bereitstellen auf dem Markt zu prüfen, ob

- das Produkt mit digitalen Elementen eine CE-Kennzeichnung trägt,
- der Hersteller und der Importeur ihren Plichten zur Beifügung der technischen Informationen und Anweisungen und der EU-Konformitätserklärung nachgekommen sind und der Importeur seinen Namen und seine Kontaktinformationen beigefügt hat.

Hat ein Händler Grund zu der Annahme, dass ein auf dem Markt bereitzustellendes Produkt mit digitalen Elementen oder die Prozesse des Herstellers zum Umgang mit Schwachstellen nicht den grundlegenden Anforderungen des Annex I entspricht, bzw. entsprechen, soll er nach Art. 14 Abs. 3 CRA-E solange von dem Bereitstellen des Produkts auf dem Markt absehen, bis die Konformität sichergestellt ist. Hat er das Produkt mit digitalen Elementen bereits auf dem Markt bereitgestellt, ist er nach Art. 14 Abs. 4 CRA-E zusätzlich verpflichtet sicherzustellen, dass die erforderlichen Abhilfemaßnahmen auch tatsächlich durchgeführt werden.

Stellt ein Händler Sicherheitsschwachstellen fest, soll er nach Art. 14 Abs. 4 CRA-E zusätzlich unverzüglich den Hersteller hierüber informieren. Folgt aus der Sicherheitsschwachstelle ein hohes Risiko für die Cybersecurity, besteht zusätzlich eine Informationspflicht der nationalen Marktüberwachungsbehörden der Mitgliedstaaten, in denen sie das Produkt mit digitalen Elementen auf dem Markt bereitgestellt hat.

5. Produktkonformität

Ein wesentlicher Baustein des Entwurfs des Cyber Resilience Act ist die Verpflichtung der Hersteller zur Durchführung von Konformitätsbewertungen. Diese Konformitätsbewertungen gelten sowohl für die Konformität der Produkte mit digitalen Elementen als auch für die Konformität der Prozesse des jeweiligen Herstellers zum Umgang mit Schwachstellen.

a) Konformitätsvermutungen

In einigen Fällen wird die Konformität von Produkten mit digitalen Elementen bzw. Prozessen der Hersteller zum Umgang mit Schwachstellen mit den grundlegenden Anforderungen des Annex I vermutet. Dies gilt nach Art. 18 Abs. 1 CRA-E zunächst, wenn und soweit die Produkte oder Prozesse mit harmonisierten Standards, die im Official Journal of the European Union veröffentlicht wurden, konform sind. Daneben wird nach Art. 18 Abs. 2 CRA-E Konformität auch dann vermutet, wenn und soweit Produkte oder Prozesse den nach Art. 19 CRA-E von der EU Kommission festzulegenden sog. common specifications entsprechen.

Eine weitere Konformitätsvermutung greift nach Art. 18 Abs. 3 CRA-E in dem Fall, dass eine EU-Konformitätserklärung oder ein EU-Zertifikat im Rahmen eines gemäß der Verordnung (EU) 2019/881 angenommenen und gemäß Art. 18 Abs. 4 CRA-E spezifizierten europäischen Cyber-Sicherheitszertifizierungssystems ausgestellt wurde.

b) Konformitätsbewertung

Wird die Konformität des Produkts mit digitalen Elementen oder den Prozessen des Herstellers zum Umgang mit Schwachstellen nicht vermutet, ist sie im Rahmen einer Konformitätsbewertung zu prüfen. Hierzu sieht Art. 24 CRA-E drei verschiedene Verfahren vor:

- ein internes Kontrollverfahren nach Annex VI, Modul A,
- eine EU-Typenprüfung nach Annex VI, Modul B gefolgt von einer Konformitätsprüfung mit EU-Typen auf der Grundlage interner Herstellungskontrolle nach Annex VI, Modul C, oder
- einer Konformitätsbewertung auf der Grundlage einer umfassenden Qualitätssicherung nach Annex VI, Modul H.

Im Falle kritischer Produkte mit digitalen Elementen nach Klasse 1, Annex III oder hochkritischer Produkte mit digitalen

Elementen nach Klasse 2, Annex III sowie den jeweils entsprechenden Prozessen der Hersteller zum Umgang mit Schwachstellen stehen nach Art. 24 Abs. 2 CRA-E, soweit keine Konformitätsvermutung greift, ausschließlich die Konformitätsbewertungsverfahren b) und c) zur Verfügung. Eine Konformitätsbewertung aufgrund interner Kontrollverfahren ist nicht möglich.

Von dieser Konformitätsprüfung nach Art. 24 CRA-E gänzlich ausgenommen werden solche Produkte mit digitalen Elementen, die als EHR-Systeme im Sinne der European Health Data Space Regulation anzusehen sind. Diese werden künftig bereits im Rahmen der European Health Data Space Regulation einem Konformitätsbewertungsverfahren unterzogen, so dass auch hier eine der eingangs erwähnten sektoralen Bereichsausnahmen greift.

Liegt nach der durchgeführten Konformitätsbewertung Produktkonformität vor, erstellt der Hersteller die EU-Konformitätserklärung (EU Declaration of Conformity) nach Maßgabe des Art. 20 CRA-E.

6. Nationale Marktüberwachungsstellen

Weiter sieht der Entwurf des Cyber Resilience Act vor, dass die Mitgliedstaaten verpflichtet werden, eine oder mehrere Marktüberwachungsstellen einzurichten, deren Zweck die Prüfung der Einhaltung der Anforderungen des Cyber Resilience Act ist. Die Wirtschaftsakteure, also die Hersteller, Importeure und Händler sind zur Mitwirkung bei derartigen Prüfungen verpflichtet.

Die Konzeption dieser Marktüberwachungsstellen ist mit den im Rahmen der NIS-Richtlinie eingeführten nationalen Behörden bzw. Anlaufstellen, die mit Aufgaben im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen beauftragt werden sollen, vergleichbar. Erachtet eine Marktüberwachungsstelle auf Grundlage einer Konformitätsprüfung ein Produkt als nicht konform, ist sie berechtigt, sofern durch andere Maßnahmen nicht ausreichend abgeholfen werden kann, den Vertrieb des Produkts zu untersagen. Dies kann bis zu einem EU-weiten Vertriebsverbot reichen.

7. Sanktionen

Für die Nichteinhaltung der durch die Verordnung auferlegten Pflichten ist ein mit der DS-GVO vergleichbares Sanktionsregime vorgesehen.

Hierbei können nach Art. 53 Abs. 3 CRA-E Bußgelder für die Nichteinhaltung der grundlegenden Sicherheitsanforderungen von bis zu 15 Mio. EUR oder 2,5 % des weltweiten Konzernjahresumsatzes des Vorjahres betragen, je nachdem, welcher Betrag höher ist. Für Verstöße gegen sonstige Verpflichtungen können nach Art. 53 Abs. 4 CRA-E Bußgelder in Höhe von bis zu 10 Mio. EUR oder 2 % des weltweiten Konzernjahresumsatzes des Vorjahres verhängt werden.

IV. Fazit

Der Cyber Resilience Act liegt zwar derzeit nur in einem Entwurfsstadium vor und wird voraussichtlich eine 12- bzw. 24-monatige Übergangsfrist beinhalten. Nichtsdestotrotz können die mit dem Cyber Resilience Act einhergehenden Verpflichtungen beträchtliche Änderungen in etablierten Prozessen bei Herstellern, Importeuren und Händler mit sich bringen. Um hohe Kosten im Rahmen der kurzfristigen oder nachträglichen Anpassung von Prozessen zu vermeiden, wird die frühzeitige Verfolgung der weiteren Entwicklungen dringend empfohlen.

Rechtsanwalt Manuel Poncza, Köln