Cyber Resilience Act: CRA

Heckmann / Paschke

2025
ISBN 978-3-406-82441-8
C.H.BECK

2. Zuordnung zum Konformitätsverfahren (Abs. 1 S. 1 2. Hs.). Bei positiver Übereinstimmung der Kernfunktion mit einer der in Anhang III erwähnten Produktkategorien formuliert Art. 7 Abs. 1 S. 1 2. Hs. als Rechtfolge für wichtige Produkte mit digitalen Elementen das Durchlaufen der **strengeren Konformitätsbewertungsverfahren** aus Art. 32 Abs. 2 oder Abs. 3. Denn während der einfache Konformitätsnachweis für die Erfüllung der grundlegenden Anforderungen aus Anhang I bei allgemeinen Produkten im Sinne von Art. 2 Abs. 1, Art. 3 Nr. 1, Nr. 2 vom Hersteller in eigener Verantwortung mithilfe des internen Kontrollverfahrens auf Grundlage von Modul A erbracht werden kann (vgl. Art. 32 Abs. 1 Buchst. a iVm Anhang VIII Teil I), erfordert das ungleich höhere Risikopotential bei wichtigen Produkten darüber hinaus das Bestehen einer zusätzlichen Vertrauenswürdigkeitsprüfung, deren Prüfungsmaßstab mit steigender Kritikalität bei wichtigen Produkten der Klasse I nach Art. 32 Abs. 2 und bei wichtigen Produkten der Klasse II nach Art. 32 Abs. 3 zunehmend strenger ausfällt. Bei Produktkategorien der Klasse I genügt nach Art. 32 Abs. 2 iVm Anhang VIII eine Selbstzertifizierung des Herstellers, wenn harmonisierte Normen, gemeinsame Spezifikationen oder europäische Zertifizierungsschemata vorhanden sind und vollständig eingehalten wurden, andernfalls ist eine notifizierte Stelle hinzuziehen (Biendl/Füllsack CR 2024, 376 (381)). **21**

Bei Produktkategorien der **Klasse II scheidet** eine **Selbstzertifizierung** hingegen aufgrund des ungleich höheren Cybersicherheitsrisikos **aus,** so dass hier gemäß Art. 32 Abs. 3 zwingend eine notifizierte Stelle beteiligt werden muss. Diese Unterteilung spiegelt einerseits den risikobasierten Ansatz des CRA wider und berücksichtigt andererseits vor dem Hintergrund des Verhältnismäßigkeitsgrundsatzes (European Commission, Impact Assessment Report, Part 1/3, S. 81 f.; Bressner/Gaden/Riediger DuD 2023, 327 (328)) den mit der Nachweiserbringung einhergehenden Verwaltungsaufwand sowie die Kostenlast des Herstellers. Dadurch kann der Hersteller die in Art. 32 Abs. 2 und Abs. 3 aufgezeigten, wenngleich auch beschränkten, Handlungsspielräume für die Nachweiserbringung der Anforderungen aus Anhang I bereits frühzeitig auf seinen Konzeptions- und Herstellungsprozess abstimmen. Allerdings verengt Art. 32 Abs. 3 bei wichtigen Produkten der Klasse II die Auswahl möglicher Nachweisinstrumente auf die Einbeziehung von Konformitätsbewertungsstellen als fachkundige und unabhängige Dritte. Dem liegt die Wertung zugrunde, dass eine unabhängige Prüfungsdurchführung bei Produkten mit hohem (Cyber-)Gefährdungspotential selbst dann gewährleistet sein muss, wenn technologisch und fachlich gut aufgestellte Hersteller den erforderlichen Konformitätsnachweis ohne Weiteres selbst mittels eigener Fähigkeiten und Ressourcen erbringen könnten. Schließlich zielt die Qualifizierung eines Produkts als wichtig im Sinne des Art. 7 Abs. 1 vorrangig darauf ab, das einschlägige Konformitätsbewertungsverfahren festzulegen, mit dem die materiellen Anforderungen aus Anhang I, die alle CRA-regulierten Produkte erfüllen müssen, überprüft werden. **22**

Das **Konformitätsverfahren** aus Art. 32 bildet den **Schwerpunkt des gesamten CRA-Regelwerks** (Zirnstein CR 2022, 707 (712)), denn es ersetzt die behördliche Präventivkontrolle (Wiebe/Daelen EuZW 2023, 257 (259)). Dessen Durchführung ist als Herstellerpflicht nach Art. 13 Abs. 12 S. 2 ausgestaltet und nicht disponibel. **23**

3. Integration wichtiger Produkte (Abs. 1 S. 2). S. 2 ordnet das Verhältnis zwischen den Produktkategorien unterschiedlicher Kritikalitätsklassen aus Anhang III sowie zwischen den allgemeinen und wichtigen Produkten. Dieser Norm- **24**

zusatz fand erst im Laufe des Gesetzgebungsverfahrens Eingang in den CRA. Den Hauptanwendungsbereich dürfte die Zusammenführung einzelner, risikoreicher Hard- oder Softwarekomponenten zu einem vernetzten Gesamtprodukt ausmachen. Wird demnach ein Produkt aus einer höheren Kritikalitätsklasse in ein Produkt aus einer niedrigeren Klasse oder ein wichtiges Produkt in ein allgemeines integriert, hat dieser Vorgang keine Auswirkungen auf die bisherige, niedrigere Kritikalitätseinstufung des Produkts, in das es integriert wird. Dies gilt unabhängig von der konkreten Funktion, die das risikoreichere Produkt im Rahmen des Zusammenwirkens ausübt. Jedes Produkt wird weiterhin isoliert nach seinem **individuellen Risikopotential** bewertet. Das Risikopotential schlägt bei zusammengesetzten Produkten nicht auf die anderen Produktbestandteile oder das Gesamtprodukt durch. Mit anderen Worten löst die Integration risikoreicher Produktkomponenten **keine Absorption** ihrer originären Kritikalitätseinstufungen durch das Gesamtprodukt aus. Infolgedessen bleibt trotz des Zusammenschlusses eines kritischeren Produkts mit einem weniger kritischen Produkt das Risikoniveau des kritikalitätsärmeren Produkts erhalten. Da im Zuge der Integration eine Erhöhung des Cybersicherheitsrisikos des Gesamtprodukts ausbleibt, bleibt die Integration auch für die Konformitätsbewertung des Gesamtprodukts folgenlos, sodass der Hersteller das strengere Produktkonformitätsverfahren aus Art. 32 Abs. 2 oder Abs. 3 nicht durchlaufen muss.

25 Diese Klarstellung erfolgt vor dem Hintergrund der **typischerweise modularen Zusammensetzung** vernetzter Produkte sowie ihrer häufigen Integration in größere Informationssysteme. Hierbei agieren einzelne Produkte als Bestandteile eines Gesamtprodukts oder -systems, indem sie aufeinander aufbauen und miteinander zusammenwirken. Dieser Zusammenhang spiegelt sich im Begriff der **Komponente** im Sinne des Art. 3 Nr. 6 wider. Komponenten können Software oder Hardware sein, die für die Integration in ein elektronisches Informationssystem bestimmt sind. Zwar findet der Begriff der Integration im CRA an unterschiedlichen Stellen Verwendung, bleibt seinerseits jedoch undefiniert. Allerdings ist bereits bei oberflächlicher Betrachtung erkennbar, dass die Begriffsbedeutung den Zusammenschluss verschiedener Komponenten zu einem einheitlichen (Gesamt-)Produkt einschließlich ihrer jeweiligen Wechselwirkungen und Abhängigkeiten in den Vordergrund rückt. Innerhalb dieser mitunter komplexen, technisch-funktionalen Gemengelage nimmt der CRA daher gezielt nur diejenigen Komponenten und Produkte isoliert in den Blick, deren Verwendung mit einem erhöhten Cybersicherheitsrisiko einhergeht. So ist eine Vielzahl der in Anhang III aufgeführten Produktkategorien bereits bestimmungsgemäß für die Integration in andere Produkte oder Informationssysteme vorgesehen. Die modulare Betrachtungsweise des CRA, die in Art. 7 Abs. 1 S. 2 zum Ausdruck kommt, verhindert damit eine konturlose Ausuferung des ohnehin breiten, sachlichen Anwendungsbereichs und stellt sicher, dass entsprechend dem gesetzgeberischen Willen lediglich ein geringer Anteil von ungefähr zehn Prozent der vom CRA regulierten Produkte der strengeren Konformitätsbewertung nach Art. 32 Abs. 2 oder Abs. 3 unterfällt.

II. Konkretisierung besonderer Eigenschaften (Abs. 2)

26 Der **Kriterienkatalog** aus Art. 7 Abs. 2 führt eine Reihe von Bewertungsaspekten auf, die die EU-Kommission heranzieht, um zu beurteilen, ob eine Aktualisierung der Produktliste aus Anhang III angezeigt ist. Damit ist der **Regelungsadressat** nicht etwa der Hersteller, der lediglich die Zuordnungsregel aus Art. 7 Abs. 1 S. 1

iVm Anhang III für die Qualifizierung eines Produkts als wichtig zu befolgen hat, sondern die **EU-Kommission,** die gemäß Abs. 3 befähigt wird, die Auflistung der Produktkategorien aus Anhang III zu verändern (Dittrich/Heinelt RDi 2023, 309 (311)). Dem Normverständnis und der Systematik allemal zuträglicher wäre daher deren Verortung ans Ende des Abs. 3 gewesen – so, wie dies bereits in der Ursprungsfassung des CRA angelegt war, vgl. Art. 6 Abs. 2 S. 2 der initialen Entwurfsfassung des CRA v. 15.9.2022 (COM(2022) 454 final). Denn aus systematischer Sicht knüpft der Regelungsinhalt unmittelbar an Abs. 3 S. 2 an, wonach die EU-Kommission gehalten ist, einen etwaigen Änderungsbedarf innerhalb der Produktkategorien aus Anhang III mithilfe einer Bewertung des zugrundeliegenden, erheblichen Cybersicherheitsrisikos der betroffenen Produktkategorien festzustellen.

Die Bestimmung der Höhe des Cybersicherheitsrisikos erfolgt dabei anhand eines oder mehrerer der in Abs. 2 unter **Buchst. a und Buchst. b** genannten Kriterien. Nach dem eindeutigen Wortlaut können sowohl die Merkmale aus Buchst. a als auch jene aus Buchst. b **gleichermaßen** herangezogen werden, um das Maß des konkreten Cybersicherheitsrisikos für die jeweilige Produktkategorie zu bestimmen und auf dieser Grundlage letztlich ihre Zuordnung zur Klasse I oder Klasse II vorzunehmen. **27**

Zugleich ermöglichen diese Bewertungsmerkmale eine weitere Konkretisierung der Eigenschaften wichtiger Produkte, ohne dass sich daraus ihre abschließende Definition herleiten lässt (Rennert ZfDR 2023, 206 (210)). Dazu trägt bei, dass selbst das Vorliegen dieser Kriterien lediglich **Indizwirkung** für die Höhe des jeweiligen, produktspezifischen Risikopotentials hat, da die Aufteilung der Kriterien in die beiden Unterkategorien gemäß Buchst. a und Buchst. b unabhängig von der Produkteinordnung in die Klasse I oder Klasse II aus Anhang III erfolgt. Zudem besteht zwischen den beiden Unterkategorien des Absatzes 2 kein Rangverhältnis, vgl. auch Erwgr. 44. Das bedeutet, dass eine Produktkategorie der Klasse I entweder alternativ oder auch kumulativ die Kriterien aus Buchst. a und Buchst. b erfüllen kann. Gleiches gilt für Produktkategorien der Klasse II. Entscheidend für die Zuweisung zur passenden Risikoklasse ist damit nicht die reine Einschlägigkeit der Kriterien aus Abs. 2, sondern das **Ergebnis** der darauf basierenden **Risikobewertung.** Dadurch kommt es entscheidend auf das Bewertungs- und Zuordnungsergebnis der Kommission an, das die Grundlage für eine Änderung der Liste aus Anhang III gemäß Abs. 3 bildet. **28**

Indessen lässt die aktuelle Zusammenstellung der Kategorienliste in Anhang III keine Rückschlüsse darauf zu, wie die Bewertungskriterien aus Abs. 2 bei der Zusammenstellung des Anhangs III konkret gewichtet werden. Es fehlen nachvollziehbare Anknüpfungspunkte zur Bestimmung der Schwere negativer Auswirkungen und damit zur Einschätzung der Höhe des Cybersicherheitsrisikos. Dieser Differenzierungsmangel und die damit verbundene, **fehlende Zuordnungsklarheit** wurden im Rahmen des Gesetzgebungsverfahren vor allem von Seiten der Wirtschaft kritisiert. Dennoch hat diese Regelungsunschärfe an dieser Stelle keine direkten Auswirkungen auf den **Hersteller,** da dieser, wie bereits erwähnt, nicht Regelungsadressat ist und daher die risikobasierte Bewertung auch nicht selbst vornehmen muss. Gleichwohl kann der Hersteller die in Abs. 2 aufgeführten Kriterien und Erwägungen, soweit zutreffend, wenigstens als **Indikatoren** für die Durchführung seiner **eigenen Bewertung** der Cybersicherheitsrisiken nutzen. Denn die Vornahme einer solchen Bewertung ist gemäß Art. 13 Abs. 2 iVm Anhang I Teil I Abs. 2 als eine zentrale Herstellerpflicht ausgestaltet und erstreckt sich auf alle, vom CRA-regulierten Produkte (Schöttle MMR 2024, 741 (744)). **29**

30 Aus dem Kriterienkatalog des Abs. 2 kann immerhin die **gesteigerte Risiko- oder Gefahrensituation** abgeleitet werden, die übergeordnete allen dort genannten Kriterien innewohnt und eine wesentliche Eigenart wichtiger Produkte darstellt. Dies lässt sich auf das hohe **Ausbreitungspotential** von Cyberdrohungen (vgl. Art. 3 Nr. 46) im Falle einer Kompromittierung wichtiger Produkte zurückführen. Die Erscheinungsformen der Cyberbedrohung im Sinne des CRA sind vielfältig und erstrecken sich auf einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte, der die Begriffsbestimmung aus Art. 2 Nr. 8 CSA übernimmt. Dieses Ausbreitungspotential hängt mit den besonderen Funktionalitäten wichtiger Produkte zusammen, die in ihren technischen Merkmalen verankert sind und dadurch den wesentlichen Grund für die Erheblichkeit des Cybersicherheitsrisikos darstellen, vgl. Art. 3 Nr. 38. Dieser Risikozusammenhang wird verstärkt durch die direkte, funktionsbezogene Software-Abhängigkeit anderer Produkte, Dienste oder Netze. Die in Buchst. a erwähnten Dienste werden nur insoweit erfasst, als dass sie Teil einer Datenfernverarbeitungslösung sind, die für den Funktionsumfang eines Produkts mit digitalen Elementen zwingend notwendig ist (vgl. Art. 3 Nr. 2 iVm Erwgr. 11), während der Begriff der Netze im Sinne einer direkten oder indirekten Datenverbindung umfassender zu verstehen ist und damit jeder Art der Vernetzung von Produkten mit digitalen Elementen erfasst (Piltz/Weiß/Zwerschke CR 2023, 154 (155)).

31 In diesem **informationstechnischen Gesamtgefüge** übernehmen wichtige Produkte für ihre vernetzte Umgebung eine Schlüsselposition, indem sie entweder eine wesentliche cybersicherheitsbezogene Funktion (Buchst. a) oder eine andere, zentrale Funktion (Buchs b.) zur Sicherstellung eines angemessenen Cybersicherheitsniveaus ausüben. Es handelt sich um technische Merkmale, aus denen ein erhebliches Cybersicherheitsrisiko resultieren kann, vgl. Art. 2 Nr. 38. Wird deren Funktionsfähigkeit beeinträchtigt, können potentielle Cybersicherheitslücken entstehen, deren Ausnutzung die Ausbreitung von Cyberbedrohungen innerhalb einzelner Software-Komponenten (systemintern) oder des gesamten vernetzten Umfelds bis hin zur gesamten Lieferkette (systemübergreifend) begünstigt. Je nach Umfang und Intensität der Ausbreitung können die daraus resultierenden, negativen Auswirkungen schwerwiegend sein. Die Einordung einer Produktkategorie in die Klasse I oder II hängt maßgeblich vom Ergebnis dieser Einschätzung ab.

32 **1. Cybersicherheitsbezogene Funktionen (Abs. 2 Buchst. a).** Die beispielhaften Merkmale in Buchst. a beschreiben unterschiedliche Ausprägungen besonderer **cybersicherheitsbezogener Funktionen**, die eine gesteigerte Kritikalität wichtiger Produkte begründen können. Deren Funktionsinhalt kann bereits unmittelbar aus ihrer Zweckbestimmung ableitet werden. Diese wird definiert als Verwendung, für die ein Produkt mit digitalen Elementen laut dem Hersteller bestimmt ist, einschließlich der besonderen Nutzungsumstände und Nutzungsbedingungen, vgl. die vollständige Definition unter Art. 3 Nr. 23. Abzustellen ist somit auf die **bestimmungsgemäße Verwendung,** die gleichzeitig die Kernfunktion wichtiger Produkte im Sinne des Art. 7 Abs. 1 S. 1 konkretisiert. Diese **Zweckbestimmung** muss gerade auf die Bereitstellung und Ausführung bedeutender Cybersicherheitsfunktionen für andere Produkte abzielen. Nichts anderes ist mit dem Wortlaut „in erster Linie" gemeint, da es sich bei den genannten Beispielen der „Sicherung der Authentifizierung und des Zugangs", der „Prävention und Erkennung von Eindrin-

gen“ sowie der „Endpunktsicherheit“ oder des „Netzschutzes“ typischerweise um wesentliche, wenngleich in dieser Form auch sehr weit formulierte Funktionalitätsmerkmale handelt, die zur Aufrechterhaltung der Cybersicherheit anderer Produkte angewendet werden. Wichtige Produkte, die bestimmungsgemäß wesentliche Cybersicherheitsfunktionen für ihr vernetztes Umfeld übernehmen, sichern das **Vertrauen** in die störungsfreie Funktionsfähigkeit ebendieser Umgebung ab.

An dieser Stelle ist es der **deutschen Textfassung** und ihrer wortlautnahen Übersetzung geschuldet, dass die genannten, cybersicherheitsbezogenen **Begrifflichkeiten** auf den ersten Blick bisweilen **schwer zugänglich** sind. Ein Vergleich mit der englischen Textfassung klärt jedoch schnell auf, dass es sich hierbei um die allgemein bekannten, technischen Maßnahmenkategorien authentication and access, intrusion prevention and detection, endpoint security sowie network protection handelt, deren englischsprachige Bezeichnung in der Praxis weit verbreitet ist. Hingegen hängt ihre inhaltliche Ausgestaltung mitunter stark vom jeweiligen informationstechnischen Einsatzumfeld ab. **33**

Ausgehend von einer allgemeinen und stark verkürzten Betrachtung lässt sich die Zweckbestimmung der in Buchst. a genannten, cybersicherheitsbezogenen Funktionalitäten wie folgt zusammenfassen: **34**

- Authentication and access (Sicherung der Authentifizierung und des Zugangs) beschreibt einen Prozess, beim dem im Rahmen der systemseitigen Zugangskontrolle mittels einer Authentifizierung die Identität eines Benutzers verifiziert wird, um diesem den Zugriff auf eine Systemressource zu gewähren oder zu verweigern.
- Intrusion prevention and detection (Prävention und Erkennung von Eindringen) kombiniert zwei Maßnahmen zur Sicherstellung der Netzwerksicherheit. Ein Intrusion-Detection-System (IDS) bezeichnet einen Prozess zur aktiven Überwachung von Softwaresystemen und -netzen, um Cyberbedrohungen frühzeitig zu erkennen und zu melden. Es kann durch ein Intrusion-Prevention-System (IPS) ergänzt werden, um ggf. durch Echtzeitanalysen des Netzwerkdatenverkehrs zusätzlich vorbeugende Maßnahmen zur Abwehr potentieller Cyberbedrohungen einzuleiten.
- Endpoint security (Endpunktsicherheit) verhindert mittels unterschiedlicher, technischer Maßnahmen den unbefugten Zugriff sowie die Ausführung schädlicher Software auf unterschiedlichen Endgeräten (vgl. Art. 3 Nr. 11), die mit einem Netzwerk verbunden sind.
- Network security (Netzschutz) bündelt diverse Prozesse und Technologien, um Produkte, Informationen und Nutzer eines Netzwerks vor vielfältigen, externen Cyberbedrohungen zu schützen. Unabhängig von der zugrundeliegenden Komplexität des zu schützenden Zielnetzwerks liegt der Fokus auf dem Auffinden von Schwachstellen sowie der Verhinderung einer Verbreitung von Cyberbedrohungen und unautorisierter Zugriffe.

Diese weit gefassten Ausprägungen wesentlicher, cybersicherheitsbezogener Funktionen treffen damit auf eine Reihe von Produktkategorien der Klasse I und der Klasse II aus Anhang III zu. Darüber hinaus deutet etwa Erwgr. 43 an, dass etwa Bootmanager als eine Produktkategorie der Klasse I ebenso über Cybersicherheitsfunktionen verfügen, deren Kompromittierung zu einer Ausbreitung von Cyberbedrohungen über die gesamte Lieferkette und damit zu schwerwiegenden nachteiligen Auswirkungen führen kann. Hieraus wird deutlich, dass allein aus der jeweiligen Zweckbestimmung, dh dem Vorhandensein einer wesentlichen Cybersicherheitsfunktion, noch keine sichere Zuweisung zu einer der beiden Risikoklas- **35**

sen aus Anhang III möglich ist. Aus diesem Grund eignet sich die Aufzählung derart allgemeiner, cybersicherheitsbezogener Funktionalitätsmerkmale nur bedingt zur Konkretisierung des spezifischen Risikopotentials wichtiger Produkte. Aufgrund dessen muss zusätzlich zu diesem Anhaltspunkt noch das besondere Potential für eine Ausbreitung möglicher Cyberbedrohungen infolge der Kompromittierung dieser Cybersicherheitsfunktionalitäten festgestellt werden.

36 Dahinter steht die Erwägung, dass der Einsatz solcher Produkte maßgeblich der Gewährleistung der klassischen Schutzziele der IT-Sicherheit, namentlich der Verfügbarkeit, Authentizität, Integrität sowie Vertraulichkeit von Informationen (vgl. Art. 3 Nr. 37) der mit ihnen verbundenen Produkte mit digitalen Elementen dient. Auch vor diesem Hintergrund lassen sich die Kriterien aus Buchst. a **nicht trennscharf** voneinander **abgrenzen,** da sie sich im Hinblick auf ihre Funktions- und Zielrichtung gegenseitig ergänzen und auch überschneiden.

37 Es bleibt festzustellen, dass infolge der Überwindung zentraler Cybersicherheitsfunktionen bei wichtigen Produkten im Sinne von Buchst. a die Angriffsfläche der mit ihnen vernetzten Umgebung potentiell erhöht wird, weil wesentliche Schutzmechanismen zur Verhinderung oder Eindämmung von Cyberbedrohungen beeinträchtigt werden oder gänzlich entfallen, wodurch eine ungehinderte Ausbreitung von Cyberbedrohungen innerhalb eines Produktes oder ganzen Netzwerks drohen kann.

38 Obwohl Umfang und Intensität einer solchen unkontrollierten Ausbreitung durchaus das Potential besitzen, schwerwiegende negative Auswirkungen hervorzurufen, werden die meisten Produktkategorien, die unter Buchst. a fallen, in der risikoärmeren Klasse I in Anhang III geführt. Beispielhaft hierfür kann zudem die in Erwgr. 10 beschriebene, verbraucherzentrierte IoT-Anwendungsdomäne smart home bemüht werden. Dort interagieren wichtige Produkte in unterschiedlichen Erscheinungsformen und -bereichen mit ihrer vernetzten Umgebung, etwa als intelligente Haushaltsgeräte mit Sicherheitsfunktionen, wie intelligente Türschlösser, Babyphone-Systeme und Alarmanlagen, vernetztes Spielzeug und am Körper tragbare medizinische Geräte (Wearables). Diese Produktkategorien werden in Anhang III ebenfalls der Klasse I zugeordnet.

39 Somit hält die Konkretisierung auf Ebene des Art. 7 Abs. 2 Buchst. a keine abgrenzungsscharfe Kategorienzuordnung bereit, womit eine **beachtliche Ungewissheit** darüber verbleibt, welche konkreten Bewertungsaspekte die Zuweisung zur Klasse I oder Klasse II auslösen.

40 **2. Weitere, risikoerhöhende Funktionen (Abs. 2 Buchst. b).** Die Aufzählung unter Buchst. b stellt auf weitere technische Merkmale wichtiger Produkte ab, die Anhaltspunkte für eine erhebliche Steigerung des Cybersicherheitsrisikos bilden. Ihre risikoerhöhende Eigenschaft resultiert, wie auch bei den Kriterien unter Buchst. a, aus einer unmittelbaren Software-Abhängigkeit anderer Produkte von den besonderen Funktionen wichtiger Produkte und der damit verbundenen Ausbreitungsgefahr im Falle der Ausnutzung von Cybersicherheitslücken, die wiederum schwerwiegende nachteilige Auswirkungen haben kann. Wie auch für die Kriterien unter Buchst. a charakteristisch, droht eine **Streuung negativer Auswirkungen** und somit eine Vergrößerung der Angriffsfläche außerhalb des angegriffenen wichtigen Produkts. Statt einer Definition solcher besonderen Risikomultiplikatoren bedient sich Buchst. b einer beispielhaften und nicht abschließenden Aufzählung von Merkmalen, die risikosteigernde Funktionen kennzeichnen und weiter konkretisieren sollen. Dazu zählt neben den zentralen Systemfunktionen,

wie etwa dem Netz(werk)management, der Konfigurationskontrolle sowie der Virtualisierung auch die Verarbeitung personenbezogener Daten.

Die Gemeinsamkeit der Eigenschaften aus dem ersten Teil der Aufzählung liegt in ihrer **grundsätzlichen Bedeutung** für die IT-Infrastruktur vernetzter Produkte, da sie weitreichende Zugriffsmöglichkeiten auf Technik und Ressourcen im Rahmen ihrer Administration, Verwaltung, Steuerung oder ihres Betriebs bieten. Hierfür sind privilegierte Zugriffsrechte erforderlich, die über Standardnutzungseinstellung hinausgehen. So können Funktionen im Bereich des Netzwerkmanagements und der Konfigurationskontrolle die Leistung und die Komponenten eines Netzwerks sowie deren Konfigurationseinstellungen verwalten, protokollieren, analysieren und überwachen. Mithilfe der (Netzwerk-)Virtualisierung können vernetzte (Software-)Ressourcen bedarfsgerecht, flexibel und zuverlässig eingesetzt werden. Diese Eigenschaften kamen in der initialen Entwurfsfassung des Art. 6 Abs. 2 Buchst. a v. 15.9.2022 (COM(2022) 454 final) deutlicher zum Ausdruck. Aufgeführt wurden hierbei etwa der Betrieb mit oder die Verwaltung von erhöhten Privilegien, direkter oder privilegierter Zugang zu Netz- oder Rechenressourcen, Kontrolle des Zugangs zu Daten oder zu operativer Technik sowie die Netzsteuerung. Diese Merkmale gehen auch weiterhin in den konkreteren Anwendungsfällen des Art. 7 Abs. 2 Buchst. b auf. **41**

Ebenso **risikobehaftet** sind nach Buchst. b Funktionalitäten zur Verarbeitung **personenbezogener Daten.** Das begriffliche Verständnis deckt sich nach Art. 3 Nr. 47 mit der Definition personenbezogener Daten aus Art. 4 Nr. 1 DS-GVO. Dessen umfassendem Ansatz folgend, werden somit alle Informationen erfasst, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Den Begriff der Verarbeitung greift der CRA zwar nicht für eine eigene Begriffsbestimmung auf, verwendet ihn aber im Katalog der grundlegenden Anforderungen in Anhang I Teil I Buchst. g im Rahmen der Umsetzung der Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (vgl. Erwgr. 32). Es ist das erklärte Ziel des CRA bei der Festlegung horizontaler Cybersicherheitsanforderungen auch personenbezogene Daten zu (vgl. initiale Entwurfsfassung des CRA v. 15.9.2022 (COM(2022) 454 final), Begründung, S. 10), wodurch beide Verordnungen, die **DS-GVO** und der CRA, nebeneinander anwendbar bleiben (Piltz/Weiß/Zwerschke CR 2023, 154 (157 f.)). Dementsprechend sollte auch der Verarbeitungsvorgang im Sinne von Art. 4 Nr. 2 DS-GVO im Anwendungsbereich des CRA weit verstanden werden und das Erheben, Erfassen, Speichern, Verändern, Auslesen, Übermitteln, Verbreiten sowie Einschränken, Löschen oder Vernichten einschließen. **42**

Diese Merkmale müssen sich in der bestimmungsgemäßen Verwendung des wichtigen Produkts widerspiegeln. Wie auch bei Buchst. a, muss die **Zweckbestimmung** gerade auf die **Bereitstellung** und **Ausführung derartiger Funktionen** ausgerichtet sein. Überdies üben auch die in Buchst. b genannten, technischen Merkmale eine Vertrauensfunktion aus und sind im Übrigen aufgrund ihrer weitreichenden funktionsspezifischen Wirkungsweise nicht immer trennscharf von den unter Buchst. a erwähnten Cybersicherheitsfunktionen abgrenzbar. Derart zentrale Funktionen sichern die ordnungsgemäße Funktionsfähigkeit und Stabilität einer vernetzten Umgebung und der darin befindlichen Produkte ab. **43**

Aus dem Kriterienkatalog gestrichen wurden im Laufe des Gesetzgebungsverfahrens Bewertungsaspekte, die auf das Ausmaß abstellten, in dem die Verwendung von Produkten mit digitalen Elementen bereits zu materiellen oder immateriellen Verlusten oder Störungen geführt hat. Solche Merkmale könnten womöglich wei- **44**

terhin Eingang in die Risikobewertung der Kommission finden, wenn sich aus ihrer Verwirklichung Rückschlüsse auf konkrete Schadenswirkungen und gegebenenfalls die Wahrscheinlichkeit ihres Eintritts aufgrund einer Wiederholungsgefahr abschätzen lassen.

45 Zwar beschreibt Buchst. b die Ausnutzung einer Cybersicherheitslücke als eine direkte **Manipulation,** die der Störung, Steuerung oder Schädigung dient, doch ergeben sich hieraus keine neuen Anforderungen, da diese Beeinträchtigungsvarianten bereits vollständig im weiten Begriffsverständnis der Cyberbedrohung gemäß Art. 3 Nr. 46 aufgehen. Denn mit dem dortigen Verweis auf Art. 2 Nr. 8 CSA wird Cyberbedrohung als ein möglicher Umstand, ein mögliches Ereignis oder eine mögliche Handlung, verstanden, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte.

46 Schließlich muss diese Sachlage ein erhebliches Risiko nachteiliger Auswirkungen für eine große Zahl anderer Produkte, die Gesundheit, Sicherheit oder Sicherheit seiner Nutzer bergen. Bei der Aufzählung der Schutzgüter fällt zunächst eine gewisse sprachliche Inkonsistenz innerhalb der deutschen Textfassung auf, die wohl auf die wortlautnahe Übersetzung aus dem Englischen zurückzuführen ist. Dort werden die Schutzgüter in Art. 7 Abs. 2 Buchst. c CRA sowie an weiteren Stellen im CRA mit health, security or safety bezeichnet, was in der deutschen Fassung spiegelbildlich mit Gesundheit, Sicherheit und mitunter auch Unversehrtheit übersetzt wird, vgl. etwa Erwgr. 10, 43. Daran schließt sich die im deutschen Schrifttum bereits zum **allgemeinen Produktsicherheitsrecht** und mittlerweile auch zum vertraglichen Digitalrecht (Schmidt-Kessel ZfPC 2022, 117 (118)) verbreite **Diskussion** über das Verständnis des **Begriffs der Sicherheit** an – in Ermangelung einer gesetzlichen Definition (Hartmann/Klindt ZfPC 2022, 73 (73 f.)) und der stetig zunehmenden Durchdringung nahezu aller Lebensbereiche mit Informationstechnik. Von der Produktsicherheit erfasst wird jedenfalls die **safety** als funktionale Sicherheit, dh die Funktions- und Betriebssicherheit eines Systems, um negative Auswirkungen des Systems auf die Anwendungsumgebung zu vermeiden (Schutz der Umwelt vor den Systemen). Demgegenüber bildet security die klassischen Schutzziele der IT-Sicherheit ab (Schutz des Systems vor seiner Umwelt). Vor dem Hintergrund des **weiten Verständnisses der Cybersicherheit** gemäß Art. 3 Nr. 4 im Sinne einer, über die klassische Schutzzielbestimmung hinausgehenden, weit gefassten Zielbildformulierung, werden sowohl diese **beiden Ausprägungen** als auch die Verarbeitung personenbezogener Daten in den Schutzbereich des CRA **einbezogen,** vgl. auch Art. 11 iVm Erwgr. 50 (→ Art. 11 Rn. 7). Auf diese Weise wird der CRA dem zugrundeliegenden Regelungsauftrag gerecht, **umfassenden Rechtsgüterschutz** für die vielfältigen Anwendungsumgebungen von Produkten mit digitalen Elementen zu gewährleisten (ähnlich Wiebe/Daelen EuZW 2023, 257 (259)), insbesondere im Verbraucherbereich (vgl. Erwgr. 10) sowie bei besonders schutzbedürftigen Anwendergruppen, wie Kindern.

47 Die Ergänzung des klassischen, produktsicherheits- und produkthaftungsbezogenen Rechtsgüterschutzes um cybersicherheitsrelevante Aspekte kommt schließlich auch **in weiteren europäischen Regulierungsvorhaben** deutlich zum Ausdruck, namentlich in Art. 6 Abs. 1 Buchst. g iVm Erwgr. 26 GPSR (→ Art. 11 Rn. 8) sowie in Art. 7 Abs. 2 Buchst. f iVm Erwg. 32, 55 der legislativen Entschließung des Europäischen Parlaments vom 12.3.2024 zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Haftung für fehlerhafte Produkte (COM(2022)0495 – C9-0322/2022 – 2022/0302(COD)).