Amtsblatt
der Europäischen Union

DE
Reihe C

C/2026/6013

17.11.2026

MITTEILUNG DER KOMMISSION

Leitlinien der Kommission zur Anwendung der Verordnung (EU) 2024/2847 (Cyberresilienzverordnung)

(C/2026/6013)

Inhaltsverzeichnis

Seite

1. EINFÜHRUNG ... 3
   - 1.1. Die Cyberresilienzverordnung ... 3
   - 1.2. Zweck dieser Leitlinien ... 3
2. ANWENDUNGSBEREICH ... 4
   - 2.1. Inverkehrbringen ... 4
   - 2.2. Software als ein Produkt mit digitalen Elementen ... 5
   - 2.3. Computercode ... 6
   - 2.4. Kombination von Hard- und Software, die ein Produkt mit digitalen Elementen bildet ... 7
   - 2.5. Datenverbindung ... 8
   - 2.6. Komplexe Systeme ... 8
   - 2.7. Produkte mit digitalen Elementen, die vor dem Inkrafttreten der Cyberresilienzverordnung entwickelt wurden ... 9
3. FREIE UND QUELLOFFENE SOFTWARE ... 11
   - 3.1. Feststellen, ob freie und quelloffene Software in die eigene Verantwortung fällt ... 12
   - 3.2. Feststellen, ob freie und quelloffene Software auf dem Unionsmarkt in den Verkehr gebracht wird ... 13
     - 3.2.1. Erheben eines Entgelts ... 13
     - 3.2.2. Monetarisierung anderer Dienste oder das Erfordernis der Verarbeitung personenbezogener Daten ... 13
     - 3.2.3. Unterstützungsleistungen ... 14
     - 3.2.4. Spenden ... 15
     - 3.2.5. Finanzierung freier und quelloffener Software ... 15
     - 3.2.6. Zum Erreichen gemeinnütziger Ziele gegründete gemeinnützige Einrichtungen ... 16
     - 3.2.7. Integration durch andere Hersteller ... 16
   - 3.3. Verwalter quelloffener Software ... 16
     - 3.3.1. Dauerhafte Unterstützung und Gewährleistung der Brauchbarkeit freier und quelloffener Software ... 17
   - 3.4. „Contributor“ und nachgelagerte Verwendungszwecke ... 18
   - 3.5. Veranschaulichende Szenarien ... 19
4. WESENTLICHE ÄNDERUNGEN UND ERSATZTEILE ... 21
   - 4.1. Physische Reparaturen ... 22
   - 4.2. Ersatzteile ... 23
   - 4.3. Software-Aktualisierungen als wesentliche Änderungen ... 24

4.4. Folgen einer wesentlichen Änderung 27
4.4.1. Wesentliche Änderungen, die von einer anderen Person als dem ursprünglichen Hersteller vorgenommen wurden 28
4.4.2. Wesentliche Änderungen, die vom ursprünglichen Hersteller vorgenommen wurden 29
5. UNTERSTÜTZUNGSZEITRAUM 29
5.1. Wesentliche Änderungen und Unterstützungszeitraum 31
6. WICHTIGE UND KRITISCHE PRODUKTE MIT DIGITALEN ELEMENTEN 32
6.1. Kernfunktionen 33
6.2. Konformitätsbewertung für wichtige und kritische Produkte mit digitalen Elementen 36
6.3. Auswirkungen auf die Konformitätsvermutung 38
7. BEWERTUNG DER CYBERSICHERHEITSRISIKEN UND INTEGRATION VON PRODUKTEN MIT DIGITALEN ELEMENTEN UND KOMPONENTEN 41
7.1. Zur Bewertung und Behandlung von Cybersicherheitsrisiken 41
7.2. Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen, sodass angesichts der Risiken ein angemessenes Maß an Cybersicherheit gewährleistet ist 42
7.3. Risikobewertung und Sorgfaltspflicht in Bezug auf externe Abhängigkeiten und integrierte Komponenten 42
7.4. Wiederverwendung von Risikobewertungs- und Konformitätsunterlagen für Familien von Produkten mit digitalen Elementen 44
8. DATENFERNVERARBEITUNG 44
8.1. Was gilt als Datenfernverarbeitungslösung für ein Produkt mit digitalen Elementen? 45
8.1.1. Der Begriff „entfernt stattfindend“ 46
8.1.2. Würde das Produkt mit digitalen Elementen ohne eine solche Datenverarbeitung eine seiner Funktionen nicht erfüllen können? 46
8.1.3. Wurde die Software vom Hersteller oder unter dessen Verantwortung konzipiert und entwickelt? 47
8.2. Praktische und technische Auswirkungen von Datenfernverarbeitungslösungen und Rückgriff auf Lösungen Dritter 49
8.3. Anwendungsfälle für Datenfernverarbeitungslösungen 50
8.3.1. Mobile Bankanwendung 51
8.3.2. Intelligenter Thermostat 52
8.3.3. E-Reader 53
8.3.4. Industrieroboter 53
8.3.5. Mobilfunknetz 53
9. WEITERE ELEMENTE 54
9.1. Meldepflichten 54
9.2. Behandlung von Schwachstellen 56
9.2.1. Vorgelagerte Meldung und gemeinsame Nutzung von Sicherheits-Patches 56
9.2.2. Bekannte ausnutzbare Schwachstellen 57
9.2.3. Wirksame und regelmäßige Tests und Überprüfungen 58
9.3. Zusammenwirken mit anderen Rechtsvorschriften 59
9.3.1. Verordnung (EU) 2019/2144 und Verordnung (EU) Nr. 168/2013 59
9.3.2. Gültigkeit von EU-Baumusterprüfbescheinigungen (Artikel 69 Absatz 1) 59

1. EINFÜHRUNG

1.1. Die Cyberresilienzverordnung

1. Die Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 ([1]) (Cyberresilienzverordnung) trat am 10. Dezember 2024 in Kraft. Ziel der Verordnung ist es, das Cybersicherheitskonzept der Union zu stärken, sich mit Cyberresilienz auf Unionsebene zu befassen und das Funktionieren des Binnenmarkts zu verbessern und dazu einen einheitlichen Rechtsrahmen für grundlegende Cybersicherheitsanforderungen für das Inverkehrbringen von Produkten mit digitalen Elementen auf dem Unionsmarkt sowie während des Lebenszyklus eines Produkts mit digitalen Elementen festzulegen.

2. Die Cyberresilienzverordnung baut auf dem neuen Rechtsrahmen der EU auf, der in der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates und Beschluss Nr. 768/2008/EG des Europäischen Parlaments und des Rates vom 9. Juli 2008 über einen gemeinsamen Rechtsrahmen für die Vermarktung von Produkten und zur Aufhebung des Beschlusses 93/465/EWG des Rates festgelegt ist ([2]).

3. Marktüberwachung und Durchsetzung sind Aufgaben der nationalen Marktüberwachungsbehörden. Produkte mit digitalen Elementen, die in den Anwendungsbereich der Cyberresilienzverordnung fallen, unterliegen den Bestimmungen der Verordnung (EU) 2019/1020 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über Marktüberwachung und die Konformität von Produkten sowie zur Änderung der Richtlinie 2004/42/EG und der Verordnungen (EG) Nr. 765/2008 und (EU) Nr. 305/2011. Die Kommission und die Agentur der Europäischen Union für Cybersicherheit (ENISA) unterstützen die Wirtschaftsakteure und die Mitgliedstaaten bei der Anwendung der Cyberresilienzverordnung.

1.2. Zweck dieser Leitlinien

4. Gemäß Artikel 26 Absatz 1 der Cyberresilienzverordnung ist die Kommission aufgefordert, Leitlinien zu veröffentlichen, um die Wirtschaftsakteure bei der Anwendung der Verordnung zu unterstützen, wobei ein besonderer Schwerpunkt auf der Erleichterung der Einhaltung durch Kleinstunternehmen sowie kleine und mittlere Unternehmen liegt. In Artikel 26 Absatz 2 ist festgelegt, auf welche Aspekte die Kommission in den Leitlinien mindestens einzugehen hat. Dazu zählen: i) der Anwendungsbereich der Cyberresilienzverordnung (mit besonderem Schwerpunkt auf Datenfernverarbeitungslösungen und freier und quelloffener Software); ii) der Begriff „Unterstützungszeiträume"; iii) das Zusammenwirken der Cyberresilienzverordnung mit weiteren EU-Rechtsvorschriften; und iv) der Begriff „wesentliche Änderung".

5. Am 3. Dezember 2025 veröffentlichte die Kommission eine Reihe häufig gestellter Fragen (FAQ), die den Wirtschaftsakteuren dabei helfen sollen, sich auf die Umsetzung der Cyberresilienzverordnung vorzubereiten ([3]).

6. Diese Leitlinien sollen den Wirtschaftsakteuren dabei helfen, die Cyberresilienzverordnung einzuhalten, und die Tätigkeit der Marktüberwachungsbehörden, notifizierenden Behörden und notifizierten Stellen unterstützen, damit eine harmonisierte Durchsetzung der Cyberresilienzverordnung in der gesamten Union sichergestellt ist. Mit diesen Leitlinien soll nicht auf den gesamten Anwendungsbereich der Cyberresilienzverordnung eingegangen werden, sondern es soll vielmehr näher erläutert werden, warum bestimmte wichtige Bestimmungen sinnvoll sind und wie sie in der Praxis umgesetzt werden könnten. Diese Leitlinien betreffen allein die Cyberresilienzverordnung, sie gelten nicht für andere EU-Rechtsvorschriften.

([1]) ABl. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

([2]) Im Arbeitsprogramm der Kommission für 2026 ist die Vorlage eines „Europäischen Produktrechtsaktes" vorgesehen, mit dem der neue Rechtsrahmen und die Vorschriften für Marktüberwachung und Normung aktualisiert werden: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52025DC0870.

([3]) Die FAQ können über die Website zur Cyberresilienzverordnung – Umsetzung der Kommission von der entsprechenden FAQ-Website heruntergeladen werden.

7. Die einschlägigen Interessenträger, einschließlich der Sachverständigengruppe für die Cybersicherheit von Produkten mit digitalen Elementen ([4]), wurden bei der Ausarbeitung dieser Leitlinien umfassend konsultiert, darunter auch im Rahmen einer öffentlichen Konsultation zwischen dem 3. März und dem 13. April 2026 ([5]).

8. Diese Leitlinien sind für Wirtschaftsakteure oder andere Akteure, die der Cyberresilienzverordnung unterliegen, nicht bindend. Eine verbindliche Auslegung der Cyberresilienzverordnung kann nur vom Gerichtshof der Europäischen Union vorgenommen werden. Die Kommission legt dessen ungeachtet in diesen Leitlinien ihre Auslegung der Cyberresilienzverordnung dar, um die Einhaltung der Verordnung zu unterstützen und zu ihrer wirksamen Umsetzung beizutragen. Darüber hinaus enthält die vorliegende Orientierungshilfe eine Reihe von Beispielen, mit denen die Anwendung gewisser Bestimmungen veranschaulicht werden soll. Diese Beispiele sind jedoch nicht dazu bestimmt, eine Einzelfallbewertung zu ersetzen – eine solche wird stets erforderlich sein, um den Besonderheiten jedes Einzelfalls Rechnung zu tragen.

9. Im Einklang mit Artikel 26 der Cyberresilienzverordnung kann die Kommission in Erwägung ziehen, weitere Leitlinien herauszugeben, darunter auch Leitlinien für Hersteller, die der Cyberresilienzverordnung und anderen Harmonisierungsrechtsvorschriften der Union oder anderen damit zusammenhängenden Rechtsakten der Union unterliegen. In diesen Leitlinien können beispielsweise Fragen zum Zusammenspiel zwischen der Cyberresilienzverordnung und der Verordnung (EU) 2024/1689 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (KI-Verordnung) sowie der Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA) behandelt werden.

2. **ANWENDUNGSBEREICH**

2.1. **Inverkehrbringen**

10. Die Cyberresilienzverordnung gilt für Produkte mit digitalen Elementen, die auf dem Unionsmarkt bereitgestellt werden. Der Begriff „Bereitstellung auf dem Markt“ ist in Artikel 3 Nummer 22 der Cyberresilienzverordnung als „die entgeltliche oder unentgeltliche Abgabe eines Produkts mit digitalen Elementen zum Vertrieb oder zur Verwendung auf dem Unionsmarkt im Rahmen einer Geschäftstätigkeit“ definiert. Gemäß Artikel 3 Nummer 21 wird ein Produkt mit digitalen Elementen auf dem Unionsmarkt in den Verkehr gebracht, wenn es erstmalig bereitgestellt wird.

11. Die jüngste Ausgabe des 2022 veröffentlichten „Leitfadens für die Umsetzung der Produktvorschriften der EU (‚Blue Guide')“ (im Folgenden „Blue Guide“ ([6])) enthält Leitlinien, die das Verständnis der EU-Produktvorschriften und ihre einheitliche Anwendung in den verschiedenen sektorspezifischen Rechtsrahmen, die an den neuen Rechtsrahmen wie die Cyberresilienzverordnung angepasst sind, erleichtern. Im „Blue Guide“ wird darauf hingewiesen, dass die Begriffe „Inverkehrbringen“ und „Bereitstellung“ so zu verstehen sind, dass sie sich „nicht auf eine Produktart, sondern auf jedes einzelne Produkt [beziehen], unabhängig davon, ob es als Einzelstück oder in Serie hergestellt wurde“ (Abschnitt 2.3).

12. Für eher „traditionelle“ Produkte mit digitalen Elementen, die unter den neuen Rechtsrahmen fallen, wie Hardware in Form von Maschinen oder Funkanlagenprodukte mit digitalen Elementen, ist der Begriff des „Inverkehrbringens“ gut etabliert, und der „Blue Guide“ enthält weitere Hinweise zur Klärung, wann solche Produkte als in den Verkehr gebracht gelten. Die „zusammenfassenden Beispiele“ in Abschnitt 2.12 des „Blue Guide“ enthalten weitere Beispiele für den Begriff des „Inverkehrbringens“.

13. Angesichts der Art immaterieller Produkte mit digitalen Elementen, etwa eigenständige Software, ist jedoch eine weitere Orientierung dahin gehend erforderlich, wann solche Produkte mit digitalen Elementen als in den Verkehr gebracht gelten. Sobald die Herstellungsphase einer Software abgeschlossen ist und das Produkt mit digitalen Elementen potenziellen Nutzern auf dem Unionsmarkt angeboten wird, kann davon ausgegangen werden, dass der Hersteller mehrere Kopien desselben Softwareprodukts mit digitalen Elementen hergestellt und sie zum Vertrieb oder zur Verwendung bereitgestellt hat. Anders als bei materiellen Produkten mit digitalen Elementen bestehen bei eigenständiger Software keine physischen Grenzen hinsichtlich ihrer Produktion oder des Lagerbestands: Jedes

([4]) Expert Group on Cybersecurity of products with digital elements in the register of Commission expert groups and other similar entities.
([5]) Public consultation on draft Commission guidance on the Cyber Resilience Act.
([6]) Bekanntmachung der Kommission – Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 („Blue Guide“) 2022/C 247/01 (ABl. C 247 vom 29.6.2022, S. 1).

Bereitstellen der Software zum Herunterladen oder zur Verbreitung führt dazu, dass eine neue identische Kopie für den Nutzer erstellt wird. Solange diese Version der Software nicht in einer Weise geändert wird, die sich auf die Einhaltung der Cyberresilienzverordnung auswirkt, gilt das Inverkehrbringen auf dem Unionsmarkt als zum Zeitpunkt des ersten Angebots zum Vertrieb oder zur Verwendung erfolgt. Die Möglichkeit des späteren Herunterladens oder einer Distribution dieser Version des Softwareprodukts mit digitalen Elementen ist daher als ein Fall anzusehen, in dem dieses Softwareprodukt mit digitalen Elementen bereitgestellt wird ([7]).

14. Daher sollte ein eigenständiges Softwareprodukt mit digitalen Elementen als in den Verkehr gebracht gelten, wenn seine Herstellungsphase abgeschlossen ist und diese Software im Rahmen einer Geschäftstätigkeit erstmals zum Vertrieb oder zur Verwendung auf dem Unionsmarkt bereitgestellt wird. Es sollte davon ausgegangen werden, dass der Hersteller mehrere Kopien des gleichen Softwareprodukts mit digitalen Elementen gleichzeitig in den Verkehr gebracht hat. Auch wenn es sich bei mehreren Kopien der gleichen Software weiterhin um Einzelprodukte mit digitalen Elementen handelt, gelten sie als gleichzeitig in den Verkehr gebracht, unabhängig davon, wann der Besitz oder die Nutzung jeder einzelnen Kopie auf eine andere natürliche oder juristische Person übertragen wird. Stellt der Hersteller Software in verschiedenen Varianten bereit, die sich in ihren enthaltenen Komponenten, Konfigurationen oder aktivierten Funktionen unterscheiden (beispielsweise Builds für unterschiedliche Betriebssysteme oder Bündel mit unterschiedlichen Funktionspaketen), können diese Varianten nicht als mehrere Kopien des gleichen Softwareprodukts mit digitalen Elementen angesehen werden. Daher sollten sie für die Zwecke des Inverkehrbringens als eigenständige Produkte mit digitalen Elementen behandelt werden.

Beispiel 1: Am 1. Januar 2028 stellt Unternehmen A über seine Website zunächst Version 1.0.0 seiner Software X zum Vertrieb bereit. Am selben Tag kauft Kunde 1 eine Kopie der Version 1.0.0 der Software X. Am 15. Januar 2028 kauft Kunde 2 eine Kopie der Version 1.0.0 der Software X. Beide Kopien der Version 1.0.0 der Software X werden am 1. Januar 2028 in den Verkehr gebracht.

15. In Anbetracht des der Softwareentwicklung innewohnenden Wiederholungscharakters sollte ferner klargestellt werden, dass nachfolgende Iterationen eines Softwareprodukts mit digitalen Elementen als neu in den Verkehr gebracht betrachtet werden, wenn diese Iterationen als „wesentliche Änderung" eines bereits in den Verkehr gebrachten Softwareprodukts mit digitalen Elementen gelten, wie in Erwägungsgrund 41 der Cyberresilienzverordnung dargelegt. Iterationen, die nicht als wesentliche Änderungen gelten, verpflichten den Hersteller nicht zur Durchführung eines neuen Konformitätsbewertungsverfahrens und es ändert sich daher nicht das Datum des Inverkehrbringens der betreffenden Software. Näheres zum Begriff der wesentlichen Änderungen ist Abschnitt *4 Wesentliche Änderungen und Ersatzteile* zu entnehmen.

Beispiel 2: Am 1. Januar 2028 stellt Unternehmen A über seine Website zunächst Version 1.0.0 seiner Software X zum Vertrieb bereit. Am selben Tag kauft Kunde 1 eine Kopie der Version 1.0.0 der Software X. Am 15. Januar 2028 gibt Unternehmen A eine aktualisierte Version 1.0.1 der Software X heraus, die keine wesentliche Änderung darstellt. Am 30. Januar 2028 kauft Kunde 2 eine Kopie der Version 1.0.1 der Software X. Beide Kopien, sowohl jene der Version 1.0.0 als auch jene der Version 1.0.1 der Software X, gelten als am 1. Januar 2028 in den Verkehr gebracht.

16. Die Leitlinien unter den Randnummern 13, 14 und 15 gelten ausschließlich insofern, als es sich bei dem Produkt mit digitalen Elementen um eigenständige Software handelt. Dies ist beispielsweise nicht der Fall, wenn die Software mit Hardware kombiniert wird, wie in Abschnitt *2.4 Kombination von Hard- und Software, die ein Produkt mit digitalen Elementen bildet* erörtert.

2.2. **Software als ein Produkt mit digitalen Elementen**

17. In Artikel 3 Nummer 1 der Cyberresilienzverordnung ist ein Produkt mit digitalen Elementen definiert als „ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in den Verkehr gebracht werden". Solche Produkte mit digitalen Elementen fallen in den Anwendungsbereich der Cyberresilienzverordnung, wenn ihre Zweckbestimmung oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung zu einem Gerät oder Netzwerk umfasst.

([7]) Gemäß Artikel 13 Absatz 11 können die Hersteller öffentliche Softwarearchive unterhalten, die den Nutzern den Zugang zu historischen Versionen erleichtern. In diesen Fällen sind die Nutzer klar und in leicht zugänglicher Form über die Risiken im Zusammenhang mit der Verwendung nicht unterstützter Software zu informieren.

18. Folglich kann eine Reihe von Produkten mit digitalen Elementen unter die Cyberresilienzverordnung fallen, darunter: i) eigenständige Software wie Apps und Computerprogramme, unabhängig davon, ob sie digital oder physisch verbreitet wird; ii) Hardware mit eingebetteter Software (beispielsweise Geräte des Internets der Dinge, Laptops, Tablets); iii) eigenständige Hardware (beispielsweise integrierte Schaltungen, Hauptplatinen) und iv) jede Kombination von Hard- und Software, die getrennt geliefert werden, aber für den gemeinsamen Betrieb bestimmt ist.

19. Folglich fällt eigenständige Software dann in den Anwendungsbereich der Cyberresilienzverordnung, wenn sie als Produkt mit digitalen Elementen in den Verkehr gebracht wird. Es ist hilfreich, zwischen Softwareprodukten mit digitalen Elementen, die der Cyberresilienzverordnung unterliegen, und der Erbringung von Ferndienstleistungen, die nicht in den Anwendungsbereich der Cyberresilienzverordnung fallen, zu unterscheiden.

20. Software fällt dann in den Anwendungsbereich der Cyberresilienzverordnung, wenn einem Nutzer ein Softwareprodukt mit digitalen Elementen zur Verfügung gestellt wird, das von diesem Nutzer erworben wurde und das seitens des Nutzers auf einem elektronischen Informationssystem oder als Teil davon betrieben wird. Software, die heruntergeladen, installiert oder dem Nutzer auf andere Weise zur Verfügung gestellt wird und die im elektronischen Informationssystem des Nutzers ausgeführt wird, entspricht diesen Kriterien, auch wenn sie beispielsweise die Form einer Browser-Erweiterung oder einer Anwendung hat, die unter Verwendung von Webtechnologien entwickelt, aber für die lokale Ausführung bereitgestellt wurde.

21. Dagegen ist Software, die aus der Ferne ausgeführt wird und auf die der Nutzer lediglich zugreift, für sich genommen kein Produkt mit digitalen Elementen. In den Erwägungsgründen 11 und 12 der Cyberresilienzverordnung wird diese Unterscheidung getroffen und in der Art erläutert, dass die Fernverarbeitung oder -speicherung nur insoweit in den Anwendungsbereich der Cyberresilienzverordnung fällt, als sie notwendig ist, damit ein Produkt mit digitalen Elementen seine Funktionen erfüllen kann (d. h. durch Datenfernverarbeitung im Sinne von Artikel 3 Nummer 2), ohne dass sie als solche ein Produkt mit digitalen Elementen wäre. Dies ist in der Regel bei Webanwendungen der Fall, einschließlich progressiver Web-Apps, auf die ausschließlich über einen Webbrowser zugegriffen wird. Gleiches gilt für Websites: Zwar können Websites in begrenztem Umfang technisch auf dem Gerät des Nutzers betrieben und ausgeführt werden, doch geht aus Erwägungsgrund 12 der Cyberresilienzverordnung hervor, dass Websites selbst nicht als Produkte mit digitalen Elementen anzusehen sind und nur dann in den Anwendungsbereich der Cyberresilienzverordnung fallen, wenn sie die Funktionalität eines Produkts mit digitalen Elementen unterstützen, d. h. soweit sie als Datenfernverarbeitungslösungen gelten (wie in Abschnitt *8* und insbesondere *8.1.2 Würde das Produkt mit digitalen Elementen ohne eine solche Datenverarbeitung eine seiner Funktionen nicht erfüllen können?* näher erläutert).

Beispiel 3: Eine mobile Anwendung, die ein Nutzer von einem App-Store herunterlädt und auf seinem Smartphone installiert, wird dem Nutzer bereitgestellt und auf einem Gerät des Nutzers ausgeführt. Folglich ist sie ein Produkt mit digitalen Elementen. Wenn sie im Rahmen einer Geschäftstätigkeit in den Verkehr gebracht wird, kann sie in den Anwendungsbereich der Cyberresilienzverordnung fallen.

Beispiel 4: Eine Desktop-Anwendung, die mithilfe von Webtechnologien gebaut, aber für eine lokale Installation gebündelt wurde, wird dem Nutzer geliefert, auf dem Gerät des Nutzers ausgeführt und ist daher ein Produkt mit digitalen Elementen. Wenn sie im Rahmen einer Geschäftstätigkeit in den Verkehr gebracht wird, kann sie in den Anwendungsbereich der Cyberresilienzverordnung fallen.

Beispiel 5: Eine Webanwendung, auf die der Nutzer ausschließlich über einen Webbrowser zugreift, ist kein Produkt mit digitalen Elementen. Sie fällt nicht in den Anwendungsbereich der Cyberresilienzverordnung, es sei denn, sie unterstützt die Funktionalität eines Produkts mit digitalen Elementen. Dagegen ist eine Anwendung, die dem Nutzer als ein lokal installierter Client zur Verfügung gestellt und auf dem Gerät des Nutzers ausgeführt wird, ein Produkt mit digitalen Elementen. Wenn sie im Rahmen einer Geschäftstätigkeit in den Verkehr gebracht wird, kann sie in den Anwendungsbereich der Cyberresilienzverordnung fallen.

Stützt sich der Kunde zur Ausführung einer oder mehrerer ihrer Funktionen auf Datenverarbeitung aus der Ferne, die der Definition des Begriffs „Datenfernverarbeitung" entspricht, ist diese Datenverarbeitung aus der Ferne ebenfalls Teil des Produkts mit digitalen Elementen.

Beispiel 6: Eine Website, die ihren Besuchern lediglich Informationen präsentiert und die Funktionalität eines Produkts mit digitalen Elementen nicht unterstützt, ist selbst kein Produkt mit digitalen Elementen. Sie fällt folglich nicht in den Anwendungsbereich der Cyberresilienzverordnung.

2.3. **Computercode**

22. Geklärt werden sollte auch, ob Quellcode ein Softwareprodukt mit digitalen Elementen sein kann. In der Cyberresilienzverordnung ist Software als „[der] Teil eines elektronischen Informationssystems, der aus Computercode besteht" definiert (Artikel 3 Nummer 4). Computercode kann die Form von i) Maschinencode haben, also die Form einer Reihe von Befehlen, die direkt vom Prozessor eines Computers ausgeführt werden und im Binärformat geschrieben sind, oder ii) die Form von Quellcode, also die Form einer Reihe von Anweisungen und Erklärungen, die in einer Programmiersprache geschrieben sind und die kompiliert oder interpretiert werden müssen, damit sie von einem Computer ausgeführt werden können. Die in der Cyberresilienzverordnung enthaltene Definition des Begriffs „Software" umfasst beides.

23. Eine andere Frage ist, ob eine bestimmte Lieferung von Computercode bedeutet, dass damit ein Produkt mit digitalen Elementen auf dem Unionsmarkt in den Verkehr gebracht wird, was eine Lieferung im Rahmen einer Geschäftstätigkeit erfordert. Dies ist bei Quellcode häufig nicht der Fall. Beispielsweise wird für die Zwecke der Cyberresilienzverordnung im Allgemeinen nicht davon ausgegangen, dass eine natürliche oder juristische Person, die freien und quelloffenen Computercode in öffentlich zugänglichen Repositorien teilt, diesen Code auf dem Unionsmarkt in den Verkehr bringt (wie in Abschnitt *3 Freie und quelloffene Software* näher erläutert). Unfertiger Code, der während der Konzeptions- und Entwicklungsphase eines Produkts mit digitalen Elementen weitergegeben wird (beispielsweise zum Testen oder Überprüfen), gilt für die Zwecke der Cyberresilienzverordnung ebenfalls nicht als in den Verkehr gebracht, da die Phase seiner Herstellung noch nicht abgeschlossen ist. Ebenso gilt Muster- oder Democode, der als Teil von Tutorials oder Trainingsmaterialien bereitgestellt wird, für die Zwecke der Cyberresilienzverordnung nicht als in den Verkehr gebracht ([8]).

24. Stellt dagegen ein Hersteller seinen Kunden Computercode als Produkt mit digitalen Elementen zur Verfügung, so gilt dieser Code als in den Verkehr gebracht, unabhängig davon, ob es sich um Maschinencode oder Quellcode handelt ([9]).

Beispiel 7: Unternehmen A erteilt Unternehmen B Lizenzen für Quellcode für eine anpassbare interne Plattform und stellt diesen Quellcode in einer Textdatei zur Verfügung. Selbst wenn dieser Quellcode vor seiner Verwendung von Unternehmen B weiter angepasst und kompiliert werden muss, bringt Unternehmen A diesen Quellcode in den Verkehr und unterliegt daher der Cyberresilienzverordnung. Unternehmen A ist dafür verantwortlich, dass bei späteren Anpassungen und Kompilationen dieses Codes durch Unternehmen B die Cyberresilienzverordnung eingehalten wird.

2.4. **Kombination von Hard- und Software, die ein Produkt mit digitalen Elementen bildet**

25. Ob Software Teil eines Produkts mit digitalen Elementen ist, sollte nicht danach bestimmt werden, wie oder wann diese Software dem Nutzer geliefert wird, sondern danach, ob die Software angesichts der Zweckbestimmung des Produkts und seiner vernünftigerweise vorhersehbaren Verwendung erforderlich ist, damit das Produkt mit digitalen Elementen seine beabsichtigten Funktionen ausführen kann. Wenn ein Hardwareprodukt mit digitalen Elementen so konzipiert ist, dass es mit einer bestimmten Software desselben Herstellers zusammenarbeitet, um seine Funktionen auszuführen, bilden Hardware und Software zusammen das Produkt mit digitalen Elementen. Software, die erforderlich ist, um ein Produkt mit digitalen Elementen entsprechend seiner Zweckbestimmung zu betreiben, zu konfigurieren, zu steuern oder zu verwenden, ist daher Teil des Produkts mit digitalen Elementen, auch wenn sie über einen gesonderten Kanal (beispielsweise einen App-Store, einen Download-Link oder einen anderen digitalen Kanal nach dem Inverkehrbringen des Hardwareprodukts mit digitalen Elementen) beschafft wird. Ihr Inverkehrbringen erfolgt somit zum gleichen Zeitpunkt wie das Inverkehrbringen von Einheiten der Hardwareprodukte mit digitalen Elementen.

Beispiel 8: Ein Netzwerkdrucker wird als Hardwareprodukt mit digitalen Elementen in den Verkehr gebracht, während die Softwaretreiber, die erforderlich sind, um Druckaufträge zu versenden, das Gerät zu konfigurieren und den Betrieb des Druckers zu verwalten, über die Website des Herstellers zum Herunterladen zur Verfügung gestellt werden. Obwohl der Drucker und die Treiber über unterschiedliche Kanäle geliefert werden, bilden sie zusammen ein einziges Produkt mit digitalen Elementen, da der Drucker ohne Treiber seiner Zweckbestimmung nicht gerecht werden kann.

Beispiel 9: Ein Fitness-Wearable wird in den Verkehr gebracht, um die Herzfrequenz und Aktivität eines Nutzers zu messen, während eine vom Hersteller bereitgestellte Smartphone-App erforderlich ist, um die Messwerte und historische Daten anzuzeigen und die Konfiguration des Geräts zu ermöglichen. Obwohl die Anwendung über einen App-Store separat heruntergeladen wird, bilden das Wearable und die App zusammen ein einziges Produkt mit digitalen Elementen, da sie für eine gemeinsame Funktionsweise konzipiert und bestimmt sind, um die Funktionalität des Produkts mit digitalen Elementen bereitzustellen.

([8]) Es sei auch daran erinnert, dass es Herstellern nach Artikel 4 Absatz 3 gestattet ist, unfertige Software, die nicht der Verordnung entspricht, wie Alpha-Versionen, Beta-Versionen oder Vorabversionen, auf dem Markt bereitzustellen, sofern die unfertige Software nur für den Zeitraum zur Verfügung gestellt wird, der für Testzwecke und das Einholen von Rückmeldungen erforderlich ist.

([9]) Andererseits sei darauf hingewiesen, dass für die Zwecke des Produkthaftungsrechts Computercode als solcher kein Produkt darstellt und daher Hersteller, die solchen Code in den Verkehr bringen, nicht nach der Richtlinie (EU) 2024/2853 (Produkthaftungsrichtlinie) haftbar gemacht werden können. In Erwägungsgrund 13 besagter Richtlinie heißt es: „Informationen sind jedoch nicht als Produkt zu betrachten, und die Produkthaftungsvorschriften sollten daher nicht für den Inhalt digitaler Dateien wie Mediendateien oder E-Books oder den reinen Quellcode von Software gelten“. Dies schließt nicht aus, dass Hersteller nach nationalem Deliktsrecht haftbar gemacht werden können.

2.5. **Datenverbindung**

26. Gemäß Artikel 2 Absatz 1 gilt die Cyberresilienzverordnung „für auf dem Markt bereitgestellte Produkte mit digitalen Elementen, deren bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt“. Der Anwendungsbereich der Cyberresilienzverordnung ist daher nicht im bloßen Vorhandensein von Elektronik verankert, sondern in der Fähigkeit eines Produkts mit digitalen Elementen, digitale Informationen auszutauschen.

27. Zwar sind die Begriffe „logische Verbindung“ und „physische Verbindung“ in Artikel 3 bestimmt, die Begriffe „Datenverbindung“ und „digitale Daten“ sind in der Cyberresilienzverordnung jedoch nicht definiert. Daher ist es sinnvoll, den Begriff „Datenverbindung“ inhaltlich auszulegen, um den Anwendungsbereich der Cyberresilienzverordnung abzugrenzen. Diese Abgrenzung ist besonders wichtig, um Produkte mit digitalen Elementen, die nur elektrische Signale verwenden, von jenen Produkten zu unterscheiden, die in eine digitale Kommunikation eingebunden und daher Cybersicherheitsrisiken ausgesetzt sind.

28. Auf der grundlegendsten Ebene beinhaltet eine Datenverbindung die Übermittlung von Informationen in binärer Form, d. h. als eine Folge von Nullen und Einsen. Das bloße Ein- und Ausschalten eines Ausgangs (d. h. „0/1“) stellt für sich genommen keine Datenverbindung dar, wenn diese Zustände nicht dazu bestimmt sind, Daten darzustellen, oder nicht von einem digitalen Eingang gelesen werden. Damit eine Datenverbindung besteht, müssen die binären Zustände von einer Quelle bewusst als Information kodiert werden und am Bestimmungsort als Information dekodiert werden können. Mit anderen Worten, es muss einen Absender geben, der nach einem festgelegten Schema bewusst digitale Symbole erzeugt, und einen Empfänger, der in der Lage ist, diese Symbole als Daten zu interpretieren. Werden elektrische oder elektronische Signale ausschließlich verwendet, um eine Funktion auszulösen oder zu betreiben, ohne digital kodierte Informationen zu übermitteln, besteht keine Datenverbindung im Sinne der Cyberresilienzverordnung, sodass das Produkt mit digitalen Elementen nicht in den Anwendungsbereich von Artikel 2 Absatz 1 fällt.

2.6. **Komplexe Systeme**

29. Produkte mit digitalen Elementen, die in den Anwendungsbereich der Cyberresilienzverordnung fallen, können nicht nur aus einzelnen Geräten oder Softwarekomponenten bestehen, sondern auch aus komplexen Systemen, einschließlich Systemen, die aus mehreren Hardware- und Softwareelementen bestehen, die zusammenwirken, um eine bestimmte Funktion auszuführen. Wird ein solches System als ein einziges Produkt mit digitalen Elementen in den Verkehr gebracht, stellt es ein Produkt mit digitalen Elementen im Sinne der Cyberresilienzverordnung dar.

30. Solche komplexen Systeme sind häufig durch lange Entwurfs- und Entwicklungszyklen gekennzeichnet, die entsprechenden Verträge wurden möglicherweise noch vor dem Inkrafttreten der Cyberresilienzverordnung unterzeichnet, und sie weisen eine besonders lange Lebensdauer und ein hohes Maß an technischer und organisatorischer Komplexität auf. Solche Systeme, die nach dem Inkrafttreten der Cyberresilienzverordnung in den Verkehr gebracht werden sollen, basieren möglicherweise auf Komponenten, die vor dem Inkrafttreten der Cyberresilienzverordnung in den Verkehr gebracht wurden, auf bereits etablierten Architekturen oder auf weitverbreiteten Interoperabilitätsstandards, darunter Standards, auf die in anderen EU-Rechtsvorschriften oder sektorspezifischen Rahmen Bezug genommen wird. Infolgedessen kann es schwierig oder unverhältnismäßig sein, bestimmte technische Merkmale dieser Systeme ohne Beeinträchtigung ihrer Zweckbestimmung, Sicherheit, Zuverlässigkeit oder Interoperabilität mit bestehender Infrastruktur zu ändern.

31. Diese Merkmale allein führen nicht dazu, dass komplexe Systeme aus dem Anwendungsbereich der Cyberresilienzverordnung ausgeschlossen sind. Vielmehr veranschaulichen sie die Anwendung des risikobasierten Ansatzes der Cyberresilienzverordnung, der es ermöglicht, die Konformität je nach den Merkmalen und Einschränkungen des Produkts mit digitalen Elementen gemäß Artikel 13 Absatz 3 der Cyberresilienzverordnung auf unterschiedliche Weise nachzuweisen. Diese Merkmale sind Teil der Zweckbestimmung des Produkts und der Umstände seines Einsatzes und daher für die Bewertung der Einhaltung der grundlegenden Cybersicherheitsanforderungen (im Folgenden „grundlegende Anforderungen“) relevant. Insbesondere wird in Erwägungsgrund 55 ausdrücklich anerkannt, dass bestimmte grundlegende Anforderungen möglicherweise mit der Art eines Produkts mit digitalen Elementen nicht vollständig vereinbar sind. Dies kann beispielsweise der Fall sein, wenn die Einhaltung verbindliche Interoperabilitätsanforderungen oder das ordnungsgemäße Funktionieren des Systems untergraben würde.

32. Dementsprechend sind die Hersteller verpflichtet, Cybersicherheitsrisiken auf der Grundlage der in Artikel 13 Absatz 2 genannten Bewertung der Cybersicherheitsrisiken zu behandeln. Wie auch in Erwägungsgrund 55 erläutert, sind in einigen Fällen bestimmte grundlegende Anforderungen nicht anwendbar oder können nicht durch

die Umsetzung von dem Stand der Technik entsprechenden Sicherheitsmaßnahmen erfüllt werden, beispielsweise aufgrund der Zweckbestimmung des Systems, die es erfordert, dass das Produkt mit digitalen Elementen mit bestehenden Abhängigkeiten interagiert oder bestimmten Interoperabilitätsanforderungen gerecht wird. In solchen Fällen sollten die Hersteller diese spezifischen Einschränkungen ermitteln und dokumentieren, die damit verbundenen Risiken bewerten und geeignete alternative oder ausgleichende Risikominderungsmaßnahmen ergreifen, damit die Sicherheit des Produkts mit digitalen Elementen nicht gefährdet wird. Für diese Zwecke spielen sowohl die in Artikel 31 genannte technische Dokumentation als auch die in Anhang II genannten Informationen und Anleitungen für den Nutzer eine Schlüsselrolle bei der transparenten Beschreibung der ermittelten Einschränkungen, der damit verbundenen Cybersicherheitsrisiken und der ergriffenen Risikominderungsmaßnahmen. Im Einklang mit der Verpflichtung, die Risikobewertung während des Unterstützungszeitraums auf dem neuesten Stand zu halten, sollten die Hersteller auch regelmäßig neu bewerten, ob solche Einschränkungen weiterhin bestehen. Lassen sich solche Einschränkungen im Laufe der Zeit aufheben oder abschwächen, sollten die Hersteller das Produkt mit digitalen Elementen entsprechend aktualisieren, damit ein angemessenes Cybersicherheitsniveau erreicht werden kann ([10]).

Beispiel 10: Ein Hersteller bringt ein Produkt mit digitalen Elementen in den Verkehr, das unter Verwendung eines Netzwerkprotokolls mit externen Systemen kommuniziert. Im Rahmen der Anwendung der grundlegenden Anforderungen stellt der Hersteller auf der Grundlage der Bewertung der Cybersicherheitsrisiken fest, dass ein sicheres Kommunikationsprotokoll erforderlich ist, um die Vertraulichkeit und Integrität der von dem Produkt mit digitalen Elementen ausgetauschten Daten zu gewährleisten.

Ihre Zweckbestimmung umfasst jedoch auch die Interoperabilität mit bestehenden Systemen, die nur ein älteres oder weniger sicheres Protokoll unterstützen. In solchen Fällen kann der Hersteller dieses Protokoll umsetzen, wenn dies aus Gründen der Interoperabilität erforderlich ist, sofern die damit verbundenen Cybersicherheitsrisiken ermittelt und durch andere Mittel gemindert werden.

Wenn es technisch machbar ist, dass das Produkt mit digitalen Elementen sowohl das sichere Protokoll als auch das weniger sichere Protokoll unterstützt, wird vom Hersteller erwartet, dass er das sichere Protokoll implementiert und dessen standardmäßige Verwendung ermöglicht. Das weniger sichere Protokoll wäre nur dann zulässig, wenn es für die Interoperabilität erforderlich ist.

Beispiel 11: Ein Hersteller eines industriellen Automatisierungssystems erwirbt vor dem Inkrafttreten der Cyberresilienzverordnung einige Mikrocontroller. Der Hersteller nimmt die Bewertung der Cybersicherheitsrisiken für sein industrielles Automatisierungssystem vor, das nach dem Inkrafttreten der Cyberresilienzverordnung in den Verkehr gebracht werden soll. Auf der Grundlage dieser Bewertung der Cybersicherheitsrisiken erkennt der Hersteller im Zusammenhang mit der Verwendung eines dieser Mikrocontroller keine spezifischen Cybersicherheitsrisiken. Der Hersteller integriert folglich diesen Mikrocontroller in sein industrielles Automatisierungssystem und stellt sicher, dass das Produkt mit digitalen Elementen als Ganzes (also das industrielle Automatisierungssystem) die grundlegenden Anforderungen erfüllt.

2.7. **Produkte mit digitalen Elementen, die vor dem Inkrafttreten der Cyberresilienzverordnung entwickelt wurden**

33. In einigen Fällen wird ein Hersteller nach Inkrafttreten der Cyberresilienzverordnung am 11. Dezember 2027 Einheiten eines Produkts mit digitalen Elementen in den Verkehr bringen, die auf Grundlage eines Typs oder Modells hergestellt wurden, der bzw. das vor dem Inkrafttreten der Cyberresilienzverordnung konzipiert und entwickelt wurde. In solchen Fällen erfordert die Einhaltung dieser Verordnung nicht unbedingt eine Neukonzeption dieser Einheiten des Produkts mit digitalen Elementen. Der Hersteller ist verpflichtet, eine Bewertung der Cybersicherheitsrisiken gemäß Artikel 13 Absatz 2 der Cyberresilienzverordnung durchzuführen, um auf der Grundlage der Zweckbestimmung und der vernünftigerweise vorhersehbaren Verwendung des Produkts mit digitalen Elementen zu bestimmen, welche der grundlegenden Anforderungen in Anhang I Teil I auf dieses Produkt mit digitalen Elementen anwendbar sind und wie diese Anforderungen umgesetzt werden.

34. Ergibt diese Risikobewertung, dass das Produkt mit digitalen Elementen bereits geeignete und wirksame Sicherheitsmaßnahmen zur Bewältigung der einschlägigen Risiken umfasst, kann sich der Hersteller auf diese bestehenden Maßnahmen stützen, um die Einhaltung der Cyberresilienzverordnung nachzuweisen. Die Cyberresilienzverordnung selbst verpflichtet nicht dazu, neue Sicherheitsmerkmale einzuführen oder das Produkt mit digitalen Elementen neu zu konzipieren, wenn dies zum Umgang mit den ermittelten Risiken nicht erforderlich ist.

([10]) Es sei darauf hingewiesen, dass die in diesem Absatz dargelegten Erwägungen gegebenenfalls für alle in den Anwendungsbereich der Cyberresilienzverordnung fallenden Produkte mit digitalen Elementen gelten können, und nicht nur für „komplexe Systeme".

35. Dennoch unterliegt der Hersteller weiterhin den in der Cyberresilienzverordnung festgelegten Pflichten. Dazu gehört, dass vor dem Inverkehrbringen des Produkts mit digitalen Elementen sichergestellt wird, dass das anzuwendende Konformitätsbewertungsverfahren durchgeführt, die EU-Konformitätserklärung ausgestellt und die CE-Kennzeichnung angebracht wurde. Die Einhaltung dieser Anforderungen ist unabhängig davon, ob die Konzeption des Produkts mit digitalen Elementen aufgrund der Risikobewertung geändert werden musste. Für Produkte mit digitalen Elementen, die vor dem Datum des Inkrafttretens der Cyberresilienzverordnung entworfen, aber erst nach diesem Datum in den Verkehr gebracht wurden, sollte, wenn der Hersteller nicht nachweisen kann, wie die Risikobewertung in der Entwurfs- und Entwicklungsphase des Produkts mit digitalen Elementen berücksichtigt wurde, die Verpflichtung nach Artikel 13 Absatz 2 so verstanden werden, dass die Hersteller verpflichtet sind, eine Bewertung der Cybersicherheitsrisiken durchzuführen und auf dieser Grundlage nachzuweisen, dass das Produkt mit digitalen Elementen angemessene Sicherheitsmaßnahmen umfasst, um Cybersicherheitsrisiken zu minimieren, Sicherheitsvorfälle zu verhindern und ihre Auswirkungen, auch in Bezug auf die Gesundheit und Sicherheit der Nutzer, zu minimieren.

36. Dementsprechend könnten Produkte mit digitalen Elementen, die vor dem Inkrafttreten der Cyberresilienzverordnung konzipiert wurden, im Rahmen der Cyberresilienzverordnung ohne Neukonzeption in den Verkehr gebracht werden, sofern der Hersteller durch die Bewertung der Cybersicherheitsrisiken und die technische Dokumentation nachweisen kann, dass das Produkt mit digitalen Elementen im Hinblick auf seine Zweckbestimmung und seine vernünftigerweise vorhersehbare Verwendung ein angemessenes Cybersicherheitsniveau erreicht und die grundlegenden Cybersicherheitsanforderungen erfüllt.

37. Darüber hinaus ist es hilfreich, die Anwendung von Konformitätsbewertungspflichten für die Hersteller von Produkten mit digitalen Elementen zu präzisieren, die zwar nach Inkrafttreten der Cyberresilienzverordnung in den Verkehr gebracht werden, aber auf Grundlage eines Typs oder Modells hergestellt worden sind, das vor diesem Datum konzipiert und entwickelt wurde. Gemäß Artikel 13 Absatz 12 muss der Hersteller im Rahmen des einschlägigen Konformitätsbewertungsverfahrens nachweisen, dass sein Produkt mit digitalen Elementen den geltenden grundlegenden Anforderungen entspricht, und diesen Nachweis in die technische Dokumentation des Produkts aufnehmen (Anhang VII Nummer 6).

38. Die Anwendung solcher Anforderungen muss jedoch im Lichte der Bewertung der Cybersicherheitsrisiken und des Cybersicherheitsrisikoprofils des Produkts mit digitalen Elementen ausgelegt werden. Insbesondere im Fall von Produkten mit digitalen Elementen, die vor dem Inkrafttreten der Cyberresilienzverordnung konzipiert wurden (aber nach diesem Datum in den Verkehr gebracht wurden) und den Konformitätsbewertungsverfahren nach Artikel 32 Absatz 1 unterliegen, sollte die Verpflichtung zur Vorlage von Nachweisen im Rahmen des Konformitätsbewertungsverfahrens nicht so verstanden werden, dass der Hersteller Prüfergebnisse vorlegen muss, die die ursprüngliche Konzeptions- und Entwicklungsphase solcher Produkte mit digitalen Elementen abdecken, wenn aus der Risikobewertung hervorgeht, dass das Produkt mit digitalen Elementen bereits geeignete und wirksame Sicherheitsmaßnahmen umfasst, die den Risiken dieses Produkts Rechnung tragen. Dies wäre aus dem Grund entbehrlich, dass es nicht dazu beitragen würde, die Sicherheit des Produkts mit digitalen Elementen selbst zu erhöhen. Wenn unter Umständen dennoch Prüfungen erforderlich sind, wird von den Herstellern nicht erwartet, dass sie Nachweise dafür vorlegen, dass Prüfungen an allen Produktvarianten durchgeführt wurden; stattdessen können sie diese Prüfungen übergreifend für Produktfamilien mit digitalen Elementen gruppieren, wie in Abschnitt *7.4 Wiederverwendung von Risikobewertungs- und Konformitätsunterlagen für Familien von Produkten mit digitalen Elementen* näher erörtert.

39. Dennoch sollte der Hersteller nachweisen, wie er die in Anhang I Teil II festgelegten Anforderungen an die Behandlung von Schwachstellen einhält, er sollte seine Risikobewertung im Einklang mit Artikel 13 Absatz 3 auf dem neuesten Stand halten, und er sollte alle anderen in der Cyberresilienzverordnung festgelegten Pflichten erfüllen, unter anderem indem er den Nutzern Informationen und Anweisungen gemäß Artikel 13 Absatz 18 zur Verfügung stellt.

Beispiel 12: Ein Hersteller bringt einen Mikrocontroller in den Verkehr, der vor dem Inkrafttreten der Cyberresilienzverordnung konzipiert und entwickelt wurde. Der Mikrocontroller soll in eine Reihe elektronischer Produkte mit digitalen Elementen integriert werden, darunter auch Produkte mit digitalen Elementen mit Konnektivitätsfunktionen.

Bevor der Hersteller nach dem Inkrafttreten der Cyberresilienzverordnung neue Einheiten des Mikrocontrollers in den Verkehr bringt, führt er eine Bewertung der Cybersicherheitsrisiken gemäß Artikel 13 Absatz 2 durch. Auf Grundlage der Zweckbestimmung des Mikrocontrollers und seiner vernünftigerweise vorhersehbaren Verwendung ermittelt der Hersteller relevante Cybersicherheitsrisiken wie unbefugten Zugriff, Manipulation von Software oder Daten und Missbrauch verfügbarer Schnittstellen.

Das Ergebnis der Risikobewertung zeigt, dass der Mikrocontroller in seiner ursprünglichen Konzeption bereits geeignete und wirksame Sicherheitsmaßnahmen zur Behandlung der ermittelten Risiken umfasst. Der Hersteller kommt daher zu dem Schluss, dass das Produkt mit digitalen Elementen die einschlägigen grundlegenden Anforderungen in Anhang I Teil I erfüllt und dass keine Neukonzeption oder Einführung zusätzlicher Sicherheitsfunktionen erforderlich ist.

Wenn nicht nachgewiesen werden kann, wie eine Bewertung der Cybersicherheitsrisiken in der ursprünglichen Konzeptions- und Entwicklungsphase berücksichtigt wurde, dokumentiert der Hersteller eine aktuelle Bewertung der Cybersicherheitsrisiken und erläutert, wie die bestehende Konzeption und die bestehenden Maßnahmen die ermittelten Risiken mindern. Der Hersteller ist nicht verpflichtet, frühere Entwurfs- oder Prüfunterlagen neu zu erstellen, da dies nicht zur Verbesserung der Cybersicherheit des Produkts mit digitalen Elementen beitragen würde. Wenn mehrere Varianten des Mikrocontrollers auf derselben Konzeption beruhen und dasselbe Cybersicherheitsrisikoprofil aufweisen, kann sich der Hersteller auch auf repräsentative Nachweise für die betreffende Produktfamilie berufen.

Der Hersteller gewährleistet ferner die Einhaltung der in Anhang I Teil II festgelegten Anforderungen bezüglich der Behandlung von Schwachstellen, unter anderem durch die Aufrechterhaltung von Verfahren zur Behandlung und Behebung von Schwachstellen und durch die fortlaufende Überprüfung der Bewertung der Cybersicherheitsrisiken gemäß Artikel 13 Absatz 3.

Unter diesen Umständen kann der vor dem Inkrafttreten der Cyberresilienzverordnung konzipierte Mikrocontroller ohne Neukonzeption in den Verkehr gebracht werden, sofern der Hersteller durch die Bewertung der Cybersicherheitsrisiken und die technische Dokumentation nachweisen kann, dass er ein im Hinblick auf die Zweckbestimmung und die vernünftigerweise vorhersehbare Verwendung des Mikrocontrollers angemessenes Cybersicherheitsniveau erreicht und die geltenden grundlegenden Anforderungen erfüllt.

3. **FREIE UND QUELLOFFENE SOFTWARE**

40. Wie in Abschnitt *2.1 Inverkehrbringen* dargelegt, gilt die Cyberresilienzverordnung für Produkte mit digitalen Elementen, die im Rahmen einer Geschäftstätigkeit erstmals auf dem Unionsmarkt bereitgestellt (d. h. „in den Verkehr gebracht“) werden, sowie für alle nachfolgenden Fälle, in denen das gleiche Produkt mit digitalen Elementen auf dem Markt bereitgestellt wird. Im „Blue Guide“ (Abschnitt 2.2) wird klargestellt, dass unter „Geschäftstätigkeit“ die entgeltliche oder unentgeltliche Bereitstellung von Waren in einem unternehmensbezogenen Kontext zu verstehen ist, was nur von Fall zu Fall unter Berücksichtigung der Regelmäßigkeit der Bereitstellung, der Eigenschaften des Produkts, der Absichten des Lieferanten usw. geprüft werden kann.

41. Eine Lieferung im Rahmen einer Geschäftstätigkeit ist durch eine Reihe von Umständen gekennzeichnet, die im „Blue Guide“ ausführlich dokumentiert und in Erwägungsgrund 15 der Cyberresilienzverordnung dargelegt sind. Zu diesen Umständen kann gehören, dass direkt für das Produkt ein Preis verlangt wird, aber auch, „dass für technische Unterstützungsleistungen ein Entgelt verlangt wird, das nicht nur der Deckung der tatsächlichen Kosten dient, dass eine Gewinnerzielungsabsicht besteht, beispielsweise durch Bereitstellung einer Softwareplattform, über die der Hersteller andere Dienste gewinnorientiert anbietet, oder dass als Bedingung für die Nutzung die Verarbeitung personenbezogener Daten zu anderen Zwecken als der alleinigen Verbesserung der Sicherheit, Kompatibilität oder Interoperabilität der Software verlangt wird oder dass Spenden angenommen werden, die die mit der Konzeption, Entwicklung und Bereitstellung eines Produkts mit digitalen Elementen verbundenen Kosten übersteigen“ (Erwägungsgrund 15) ([11]).

42. Durch die Cyberresilienzverordnung werden jedoch die Besonderheiten der verschiedenen Arten der Entwicklung und Veröffentlichung von „freier und quelloffener Software“ anerkannt und einige Orientierungshilfen angeboten, um leichter feststellen zu können, ob es sich bei freier und quelloffener Software um ein Produkt mit digitalen Elementen handelt, das im Sinne der Cyberresilienzverordnung (d. h. im Rahmen einer Geschäftstätigkeit) in den Verkehr gebracht wird. Wie in Erwägungsgrund 18 erläutert, sollten „die bloßen Umstände, unter denen das Produkt mit digitalen Elementen entwickelt wurde, oder die Art und Weise, wie die Entwicklung finanziert wurde, … bei der Bestimmung des kommerziellen oder nichtkommerziellen Charakters der entsprechenden Tätigkeit nicht berücksichtigt werden“. Insbesondere sollte, „die Bereitstellung von Produkten mit digitalen Elementen, die als freie und quelloffene Software eingestuft und von ihren Herstellern nicht zu Geld gemacht werden, nicht als Geschäftstätigkeit betrachtet werden, damit sichergestellt ist, dass klar zwischen der Entwicklungs- und der Lieferphase unterschieden wird“.

([11]) Es sei auch daran erinnert, dass Produkte mit digitalen Elementen zwar häufig (auch) durch die Verarbeitung personenbezogener Daten monetarisiert werden, der Schutz personenbezogener Daten jedoch ein Grundrecht ist und daher personenbezogene Daten nicht als Ware betrachtet werden können, wie in Erwägungsgrund 24 der Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (ABl. L 136 vom 22.5.2019, S. 1, ELI: http://data.europa.eu/eli/dir/2019/770/oj), angegeben.

43. Daher ist es sinnvoll, i) klarzustellen, was freie und quelloffene Software ist; ii) wann davon ausgegangen wird, dass sie unter die Verantwortung einer natürlichen oder juristischen Person fällt, und iii) Beispiele aufzuzeigen, die den Interessenträgern helfen zu verstehen, wann der Vertrieb von freier und quelloffener Software ein Inverkehrbringen darstellt. Wird freie und quelloffene Software nicht in den Verkehr gebracht, fällt sie nicht in den Anwendungsbereich der Cyberresilienzverordnung, es sei denn, die Einrichtung, die sie veröffentlicht, ist eine juristische Person, die der Definition des „Verwalters quelloffener Software“ (im Folgenden „Verwalter“) gemäß Artikel 3 Nummer 14 entspricht. In diesem Fall unterliegt sie nur den Pflichten nach Artikel 24.

44. In Artikel 3 Nummer 48 ist freie und quelloffene Software definiert als „eine Software, deren Quellcode offen geteilt wird und die im Rahmen einer kostenlosen Open-Source-Lizenz zur Verfügung gestellt wird, die alle Rechte vorsieht, um sie frei zugänglich, nutzbar, veränderbar und weiterverteilbar zu machen“. Obwohl in diesen Leitlinien keine spezifischen freien und quelloffenen Lizenzen genannt werden, die mit der Definition in Artikel 3 Nummer 48 vereinbar sind, ergibt sich aus dem Wortlaut dieser Bestimmung, dass nur Software, die kumulativ zwei Bedingungen erfüllt, für die Zwecke der Cyberresilienzverordnung als freie und quelloffene Software gilt: i) Die Software muss im Rahmen einer freien und quelloffenen Lizenz zur Verfügung gestellt werden, mit der alle in Artikel 3 Nummer 48 genannten Rechte gewährt werden, und ii) ihr Quellcode muss offen geteilt werden.

45. In der Erfordernis hinsichtlich der Lizenz, dass die Software „frei zugänglich, nutzbar, veränderbar und weiterverteilbar“ sein muss, spiegelt sich das traditionelle Verständnis von freier und quelloffener Software wider, wonach die Nutzer in der Lage sein müssen, auf den Quellcode zuzugreifen, ihn ohne unangemessene Einschränkung zu verwenden, ihn zu ändern und ursprüngliche oder geänderte Versionen weiterzuverbreiten. Der Zugang zum Quellcode ist daher eine notwendige Voraussetzung für die Ausübung der anderen Rechte: Ohne Zugang zum Quellcode ist es praktisch nicht möglich, die Software zu verändern oder sinnvoll weiterzuverwenden.

46. In Artikel 3 Nummer 48 wird jedoch über die bloße Bezugnahme auf die Lizenzbedingungen hinausgegangen, da dort ausdrücklich verlangt wird, dass der Quellcode „offen geteilt wird“. Der Begriff „offen geteilt“ bedeutet, dass der Quellcode öffentlich zugänglich gemacht werden muss (entweder „vorgelagert“ oder „nachgelagert“) und nicht nur eingeschränkt oder bedingt bereitgestellt werden darf. Dementsprechend ist Software, die im Rahmen einer freien und quelloffenen Lizenz vertrieben wird, deren Quellcode jedoch nur an zahlende Kunden oder eine begrenzte Gruppe von Nutzern weitergegeben wird (oder weitergegeben werden darf), nicht als freie und quelloffene Software im Sinne von Artikel 3 Nummer 48 zu betrachten. Für die Zwecke der Cyberresilienzverordnung sollte daher nur Software, deren Quellcode öffentlich zugänglich ist und im Rahmen einer freien und quelloffenen Lizenz lizenziert wird, die alle in Artikel 3 Nummer 48 genannten Rechte gewährt, als freie und quelloffene Software gelten.

3.1. **Feststellen, ob freie und quelloffene Software in die eigene Verantwortung fällt**

47. Mit der Cyberresilienzverordnung werden den Wirtschaftsakteuren, die auf dem Unionsmarkt Produkte mit digitalen Elementen bereitstellen, zentrale Zuständigkeiten übertragen. Durch die Verordnung wird der Hersteller als die natürliche oder juristische Person definiert, die ein Produkt mit digitalen Elementen unter ihrem eigenen Namen oder ihrer eigenen Marke im Rahmen einer Geschäftstätigkeit bereitstellt (und es somit in den Verkehr bringt). Analog ist ein Einführer die in der EU ansässige natürliche oder juristische Person, die das Produkt mit digitalen Elementen einer außerhalb der EU ansässigen Person im Rahmen einer Geschäftstätigkeit liefert (und es somit in den Verkehr bringt). Die Pflichten der Verwalter gelten für die juristische Person, die eine für Geschäftstätigkeiten bestimmte freie und quelloffene Software liefert ([12]), sie aber nicht im Sinne der Cyberresilienzverordnung in den Verkehr bringt.

48. Um festzustellen, ob eine natürliche oder juristische Person freie und quelloffene Software in der EU in den Verkehr bringt, muss daher zunächst geklärt werden, ob diese natürliche oder juristische Person die freie und quelloffene Software tatsächlich liefert. Um die geltenden Pflichten im Rahmen der Cyberresilienzverordnung korrekt festzulegen, muss festgestellt werden, ob die natürliche oder juristische Person die Maßnahme der Bereitstellung einer freien und quelloffenen Software tatsächlich ausführt. Wie in Erwägungsgrund 18 dargelegt, gilt die Cyberresilienzverordnung nicht für natürliche oder juristische Personen, die mit Quellcode zu Produkten mit digitalen Elementen beitragen, die als freie und quelloffene Software eingestuft sind und nicht ihrer Verantwortung unterliegen.

([12]) Dies ist eine notwendige, nicht jedoch hinreichende Voraussetzung dafür, dass eine juristische Person als Verwalter quelloffener Software gelten kann, da in der Begriffsbestimmung in Artikel 3 Nummer 14 weitere Bedingungen festgelegt sind, unter denen eine juristische Person als Verwalter gelten kann.

49. Angesichts der Besonderheiten der Entwicklung von freier und quelloffener Software, an der häufig mehrere „Contributor“ beteiligt sind, dezentraler Kooperationsmodelle und einer Trennung zwischen Beitrag und Entscheidungsfindung ist es sinnvoll klarzustellen, dass freie und quelloffene Software als „unter der Verantwortung“ natürlicher oder juristischer Personen stehend erachtet wird, die sie veröffentlichen und die primäre Kontrolle über ihre Entwicklung, Freigabe und Vertriebsentscheidungen ausüben (häufig als „Maintainer“ bezeichnet). Personen, die Quellcode beitragen, aber keinen Einfluss auf Freigabe-, Roadmap- oder Governance-Entscheidungen haben, gelten als „Contributor“; sie tragen keine Verantwortung für die freie und quelloffene Software, obwohl sie mit Code zu ihr beigetragen haben. Die bloße Existenz technischer Genehmigungen, beispielsweise einer Zugangserlaubnis, reicht nicht aus, um nachzuweisen, dass die betreffende freie und quelloffene Software der Verantwortung dieser Person unterliegt; die Verantwortung liegt stattdessen bei jenen Personen, die die freie und quelloffene Software veröffentlichen und kontrollieren.

Beispiel 13: Ein einzelner Entwickler oder ein Mitarbeiter eines Unternehmens reicht eine „Pull-“ oder „Merge-“Anfrage mit einem Sicherheitspatch oder einer neuen Funktion für ein Projekt für eine freie und quelloffene Software ein. Die „Maintainer“ des Projekts überprüfen, akzeptieren und mergen den Code in das Main Repository und nehmen ihn anschließend in eine neue Version auf. In diesem Szenario ist die Person, die den Pull-Antrag gestellt hat, ein „Contributor“ und unterliegt nicht der Cyberresilienzverordnung. Diese Person hat zwar Quellcode beigetragen, übt aber keine primäre Kontrolle über die Entwicklungs-, Versions- oder Vertriebsentscheidungen aus.

3.2. **Feststellen, ob freie und quelloffene Software auf dem Unionsmarkt in den Verkehr gebracht wird**

50. Sobald feststeht, dass eine freie und quelloffene Software unter der Verantwortung einer natürlichen oder juristischen Person steht, muss festgestellt werden, ob diese Person diese Software im Rahmen einer Geschäftstätigkeit liefert und diese Transaktion folglich ein Inverkehrbringen darstellt.

3.2.1. *Erheben eines Entgelts*

51. Stellt die natürliche oder juristische Person, die freie und quelloffene Software liefert, einen Preis für die Software selbst in Rechnung (beispielsweise durch Erhebung eines Entgelts für die vorkompilierten Binärdateien), so bringt diese Person ein Produkt mit digitalen Elementen in den Verkehr. Die Person, die eine freie und quelloffene Software in den Verkehr bringt, ist daher ein Hersteller im Sinne der Cyberresilienzverordnung.

52. Häufig liefern Hersteller von freier und quelloffener Software kostenlos Versionen diese Software (häufig als „Community-Versionen“ bezeichnet), deren Codebase (fast) identisch mit der kostenpflichtigen Version ist. Bei diesen Produkten mit digitalen Elementen handelt es sich jedoch um unterschiedliche Produkte: Die kostenpflichtige Version wird in irgendeiner Weise monetarisiert (beispielsweise durch die Erhebung eines Entgelts oder auf andere Weise, wie in diesem Abschnitt erörtert) und gilt daher als in den Verkehr gebracht, wodurch die Pflichten des Herstellers wirksam werden. Die kostenlos bereitgestellte Version (oder „Community-Version“) wird nicht monetarisiert und gilt daher im Sinne der Cyberresilienzverordnung als nicht in den Verkehr gebracht. Dies ist auch der Fall, wenn es sich bei der kostenpflichtigen Version um eine „erweiterte“ kommerzielle Version handelt, durch welche die Codebasis der kostenlos bereitgestellten Version erweitert oder diese Version in ein breiteres Produkt mit digitalen Elementen integriert wird (wie es beispielsweise beim „Open-Core-Modell“ der Fall ist).

53. Handelt es sich bei der Person, die die Community-Version bereitstellt, um eine juristische Person, so unterliegt diese juristische Person auch für diese kostenlos bereitgestellte Version (die Community-Version) den Pflichten der Verwalter. Wird die kostenlose Version (die Community-Version) hingegen von einer natürlichen Person bereitgestellt, fällt sie nicht in den Anwendungsbereich der Cyberresilienzverordnung.

3.2.2. *Monetarisierung anderer Dienste oder das Erfordernis der Verarbeitung personenbezogener Daten*

54. Eine natürliche oder juristische Person, die eine freie und quelloffene Software veröffentlicht, kann diese auch in den Verkehr bringen (d. h. im Rahmen einer Geschäftstätigkeit liefern), wenn über die bereitgestellte Software andere Produkte mit digitalen Elementen oder Dienstleistungen monetarisiert werden, oder wenn sie als Voraussetzung für die Nutzung der Software die Verarbeitung personenbezogener Daten aus anderen Gründen als ausschließlich zur Verbesserung der Sicherheit, Kompatibilität oder Interoperabilität der Software verlangt.

Beispiel 14: Eine natürliche oder juristische Person veröffentlicht eine kostenlose und quelloffene Marktplatzanwendung. Die Anwendung ist kostenlos verfügbar und ermöglicht es den Nutzern, darüber Waren oder Dienstleistungen zu kaufen. Sie ermöglicht es der Person, die sie veröffentlicht hat, darüber angebotene andere Produkte mit digitalen Elementen sowie Dienstleistungen zu monetarisieren (beispielsweise durch Werbung, Provisionen oder Abonnementgebühren). Folglich gilt die Anwendung als im Rahmen einer Geschäftstätigkeit in den Verkehr gebracht.

Beispiel 15: Eine natürliche oder juristische Person veröffentlicht ein kostenloses und quelloffenes VPN. Die Anwendung ist kostenlos verfügbar, allerdings haben die Nutzer die Möglichkeit, gegen Bezahlung auf zusätzliche Server oder spezielle IP-Adressen zuzugreifen. Die Anwendung ermöglicht also dem Anbieter, andere darüber angebotene Dienste zu monetarisieren, weshalb sie als im Rahmen einer Geschäftstätigkeit in den Verkehr gebracht gilt.

Beispiel 16: Eine natürliche oder juristische Person veröffentlicht eine kostenlose und quelloffene Fitness-Tracking-Anwendung. Die Anwendung ist kostenlos verfügbar, Voraussetzung für ihre Nutzung ist jedoch die Verarbeitung personenbezogener Daten der Nutzer für solche Zwecke wie gezielte Werbung oder Analysen, die in keinem Zusammenhang mit der Sicherheit, Kompatibilität oder Interoperabilität der Software stehen. Wenn eine solche Form der Datenverarbeitung als Nutzungsbedingung vorgeschrieben wird, gilt die Anwendung als im Rahmen einer Geschäftstätigkeit in den Verkehr gebracht.

3.2.3. *Unterstützungsleistungen*

55. Die bloße Tatsache, dass eine natürliche oder juristische Person, die eine freie und quelloffene Software veröffentlicht, auch damit verbundene entgeltliche Unterstützungsleistungen anbietet, bedeutet nicht zwingend, dass das Produkt mit digitalen Elementen im Rahmen einer Geschäftstätigkeit bereitgestellt wird. Unterstützungsleistungen können Tätigkeiten wie Beratung, Training oder professionelle Dienstleistungen im Zusammenhang mit der Nutzung, Dokumentation, Konfiguration und dem Einsatz der Software durch einen Kunden umfassen.

56. Entscheidend ist, ob der eigentliche Zugang zu der freien und quelloffenen Software (d. h. die Bereitstellung des Produkts mit digitalen Elementen), einschließlich seiner Wartung, an eine Vergütung geknüpft ist, und nicht an das bloße Anbieten professioneller Dienstleistungen rund um ein frei verfügbares Produkt mit digitalen Elementen, wie in Erwägungsgrund 18 der Cyberresilienzverordnung dargelegt („die Bereitstellung von Produkten mit digitalen Elementen, die als freie und quelloffene Software eingestuft und von ihren Herstellern nicht zu Geld gemacht werden, [sollte] nicht als Geschäftstätigkeit betrachtet werden"). Wenn freie und quelloffene Software kostenlos heruntergeladen und installiert werden kann und die Nutzer sich freiwillig dafür entscheiden können, professionelle Dienstleistungen separat zu erwerben, gilt diese Software nicht als in den Verkehr gebracht.

57. Im Gegensatz dazu ist der Zugang zu einer bestimmten Version eines Produkts mit digitalen Elementen, die bestimmte Vorteile wie technische Hilfe oder Leistungsoptimierung umfasst, mitunter von einer Vergütung abhängig. In solchen Fällen stellt diese Bestimmung eine entgeltliche Bereitstellung eines Produkts mit digitalen Elementen dar, das im Rahmen einer Geschäftstätigkeit bereitgestellt wird, und folglich gilt das Produkt in den Verkehr gebracht. Dies gilt auch für Fälle, in denen eine kostenpflichtige Ausgabe oder Unternehmensversion im Rahmen einer gewerblichen Vereinbarung zur Verfügung gestellt wird, unabhängig davon, ob funktionsäquivalente Software auch im Rahmen einer freien und quelloffenen Lizenz kostenlos zur Verfügung steht.

Beispiel 17: Eine natürliche oder juristische Person veröffentlicht ein freies und quelloffenes Betriebssystem, wobei gleichzeitig eine kostenpflichtige Version dieses Betriebssystems angeboten wird, die Unterstützungsdienste wie technische Hilfe oder Leistungsoptimierung umfasst. Die kostenpflichtige Version des Betriebssystems gilt als im Rahmen einer Geschäftstätigkeit in den Verkehr gebracht.

Beispiel 18: Eine natürliche oder juristische Person veröffentlicht ein kostenloses und quelloffenes Befehlszeilentool. Das Tool ist frei zugänglich und kann von jedermann heruntergeladen und installiert werden. Diese natürliche oder juristische Person bietet separat professionelle Dienstleistungen an, beispielsweise optionale Beratungsdienste zur Schulung von Nutzern sowie zur Unterstützung bei der Installation und Nutzung des Tools. Diese freie und quelloffene Software gilt im Sinne der Cyberresilienzverordnung nicht als in den Verkehr gebracht.

58. Insbesondere im Falle natürlicher Personen, die freie und quelloffene Software veröffentlichen, würde das Angebot technischer Hilfe, direkt im Paket mit dem Zugang zu dem Produkt mit digitalen Elementen, noch immer nicht als Geschäftstätigkeit gelten, wenn, wie in Erwägungsgrund 15 der Cyberresilienzverordnung dargelegt, der in Rechnung gestellte Preis nur der Deckung der tatsächlichen Kosten dient. Diese tatsächlichen Kosten umfassen eine Vielzahl von Kosten im Zusammenhang mit der Konzeption, Entwicklung und Wartung dieser Software, einschließlich der angemessenen Lebenshaltungskosten der betreffenden Person. Wenn also eine natürliche Person eine freie und quelloffene Software veröffentlicht und technische Unterstützung anbietet, um ihre Kosten zu decken und eine angemessene Vergütung zu erhalten, kann nicht allein auf dieser Grundlage davon ausgegangen werden, dass diese Person die betreffende Software in der EU in den Verkehr gebracht hat.

59. Bei einer natürlichen oder juristischen Person, die technische Unterstützung im Zusammenhang mit einer freien und quelloffenen Software anbietet, für die sie nicht verantwortlich ist, wird nicht davon ausgegangen, dass sie diese Software in den Verkehr bringt, es sei denn, diese Person nimmt im Rahmen solcher Unterstützungsleistungen eine wesentliche Änderung an der freien und quelloffenen Software gemäß Artikel 22 vor.

Beispiel 19: Ein Dienstleister veröffentlicht keine freie und quelloffene Software, sondern hilft einem Kunden dabei, eine solche Software auf dem Server des Kunden in dessen Räumlichkeiten zu installieren. Dabei nimmt der Dienstleister keine wesentliche Änderung an dieser freien und quelloffenen Software vor. Folglich wird nicht davon ausgegangen, dass der Dienstleister die freie und quelloffene Software in den Verkehr bringt.

3.2.4. *Spenden*

60. Natürliche oder juristische Personen, die Projekte mit freier und quelloffener Software veröffentlichen, bieten Nutzern dieser Software regelmäßig Möglichkeiten, freiwillig Geld zu spenden, um dem/den Herausgeber(n) des Projekts zu danken und sicherzustellen, dass das Projekt aktiv fortgeführt wird.

61. In Erwägungsgrund 15 der Cyberresilienzverordnung heißt es: „Die Annahme von Spenden ohne Gewinnabsicht sollte nicht als Geschäftstätigkeit gelten." Die bloße Aufnahme eines Links zu einer Spendenplattform oder ähnlichen Tools zur Spendensammlung sollte nicht als Gewinnabsicht angesehen werden, selbst wenn der durch Spenden eingenommene Betrag die reinen Kosten im Zusammenhang mit der Konzeption, Entwicklung und Bereitstellung eines Produkts mit digitalen Elementen übersteigt. Diese Kosten umfassen auch eine angemessene Bezahlung der von einer juristischen Person eingestellten Mitarbeiter und/oder die angemessenen Lebenshaltungskosten einer natürlichen Person. Spenden schwanken naturgemäß im Laufe der Zeit, weshalb bei der Beurteilung, ob eine ausschließlich durch Spenden monetarisierte freie und quelloffene Software als in den Verkehr gebracht gilt, ein gewisses Maß an Flexibilität erforderlich ist. Es ist daher unwahrscheinlich, dass eine freie und quelloffene Software, die nur durch Spenden unterstützt wird, im Sinne der Cyberresilienzverordnung als in den Verkehr gebracht zu erachten ist.

Beispiel 20: Eine natürliche oder juristische Person veröffentlicht eine freie und quelloffene Software in einem öffentlichen Online-Repository, sodass es jedermann möglich ist, diese Software im Rahmen einer kostenlosen und quelloffenen Lizenz herunterzuladen, zu nutzen, zu ändern und weiterzuverbreiten. Die Nutzer werden vom Herausgeber der Software aufgefordert, über eine Spendenplattform freiwillig Spenden zu leisten, um die Weiterentwicklung und Pflege des Projekts zu unterstützen. Der Zugang zu der Software, ihrem Quellcode und ihren Aktualisierungen ist nicht von einer Spende abhängig. Folglich gilt diese freie und quelloffene Software nicht als im Rahmen einer Geschäftstätigkeit bereitgestellt und auch nicht als im Sinne der Cyberresilienzverordnung in den Verkehr gebracht.

62. Dennoch gibt es Fälle, in denen eine durch Spenden unterstützte freie und quelloffene Software als in den Verkehr gebracht gelten kann. Dies ist beispielsweise der Fall, wenn auf der Grundlage einer Gesamtbewertung der Umstände die Spenden de facto der Erhebung eines Entgelts für den Zugang zu dem Produkt mit digitalen Elementen oder bestimmten seiner Funktionen gleichzusetzen sind. Dies kann insbesondere dann der Fall sein, wenn der Zugang zur freien und quelloffenen Software, zu wesentlichen Funktionen oder zu Aktualisierungen in der Praxis von einer Spende abhängig gemacht wird oder wenn Spenden mit vertraglichen Vergünstigungen oder ausschließlichen Vorteilen verbunden sind, die über die Vorteile für die Gemeinschaft hinausgehen.

Beispiel 21: Eine natürliche oder juristische Person veröffentlicht ein Softwareprodukt mit digitalen Elementen im Rahmen einer kostenlosen und quelloffenen Lizenz, stellt aber herunterladbare Versionen und Sicherheitsaktualisierungen nur Nutzern zur Verfügung, die eine Spende leisten. Wer nichts spendet, hat keinen Zugang zur aktuellen Version der Software.

In diesem Fall sind die Spenden de facto eine Voraussetzung für den Zugang zu dem Produkt mit digitalen Elementen und stellen daher die Erhebung eines Entgelts dar. Diese freie und quelloffene Software gilt folglich im Sinne der Cyberresilienzverordnung als in den Verkehr gebracht.

Beispiel 22: Eine natürliche oder juristische Person macht den Quellcode einer freien und quelloffenen Software öffentlich zugänglich, stellt jedoch vorkompilierte Binärdateien, regelmäßige Aktualisierungen sowie das garantierte Beseitigen von Sicherheitslücken nur für Spender bereit. In diesem Fall sind die Spenden mit dem Zugang zu wesentlichen Aspekten des Produkts mit digitalen Elementen verbunden und stellen eine Vergütung für die Bereitstellung dieses Produkts dar. Diese freie und quelloffene Software gilt folglich als im Rahmen einer Geschäftstätigkeit in den Verkehr gebracht.

3.2.5. *Finanzierung freier und quelloffener Software*

63. Die bloße Tatsache, dass ein Dritter für die Entwicklung freier und quelloffener Software bezahlt, eine Spende geleistet oder die Entwicklung auf andere Weise finanziert hat, ist als solche nicht ausschlaggebend dafür, ob die betreffende freie und quelloffene Software in den Verkehr gebracht wird. Im Ökosystem freier und quelloffener Software ist es gängige Praxis, dass einzelne Entwickler, Stiftungen oder Gemeinschaften Finanzmittel von Unternehmen, öffentlichen Stellen oder anderen Sponsoren erhalten, um an bestimmten Funktionen zu arbeiten, Fehler zu beheben oder kritische Komponenten zu unterhalten. Diese Finanzierung kann viele Formen annehmen, darunter Zuschüsse, „Bug-Bounty"-Programme, Sponsoring, Dienstleistungsverträge oder bezahlte Entwicklungsarbeit.

64. Wie bereits erwähnt, wird in Erwägungsgrund 18 der Cyberresilienzverordnung klargestellt, dass die bloßen Umstände, unter denen das Produkt mit digitalen Elementen entwickelt wurde, oder die Art und Weise, wie die Entwicklung finanziert wurde, bei der Bestimmung des kommerziellen oder nichtkommerziellen Charakters der entsprechenden Tätigkeit nicht berücksichtigt werden sollten.

65. Daher sollte in Fällen, in denen freie und quelloffene Software offen geteilt und allen frei zugänglich gemacht wird, um auf die Software zugreifen, sie nutzen, ändern und weiterverbreiten zu können, die Tatsache, dass eine gewerbliche Rechtsperson möglicherweise für das betreffende Projekt bezahlt hat, bei der Feststellung, ob die Software in den Verkehr gebracht wird, keine Rolle spielen. Wenn diese freie und quelloffene Software nicht anderweitig monetarisiert wird, ist sie nicht als in den Verkehr gebracht anzusehen. Wenn das Unternehmen, das die Entwicklung der freien und quelloffenen Software finanziert hat (sowie jedes andere Unternehmen), diese in sein Produkt mit digitalen Elementen integriert, muss dieses Unternehmen seiner Sorgfaltspflicht gemäß Artikel 13 Absatz 5 der Cyberresilienzverordnung nachkommen.

Beispiel 23: Ein einzelner Entwickler veröffentlicht ein Projekt mit freier und quelloffener Software und betreut es aktiv. Hersteller A wünscht, dass der einzelne Entwickler diese freie und quelloffene Software um eine spezifische Funktion erweitert, und bezahlt diese Entwicklungsleistung. Der Entwickler erweitert die Codebasis der freien und quelloffenen Software, teilt sie offen und macht sie für alle frei zugänglich, sodass alle auf sie zugreifen, sie nutzen, ändern und weiterverbreiten können. In diesem Fall wird nicht davon ausgegangen, dass der einzelne Entwickler diese freie und quelloffene Software in den Verkehr gebracht hat. Wenn der Hersteller die freie und quelloffene Software in sein Produkt mit digitalen Elementen integriert, muss er seiner Sorgfaltspflicht gemäß Artikel 13 Absatz 5 genügen.

3.2.6. *Zum Erreichen gemeinnütziger Ziele gegründete gemeinnützige Einrichtungen*

66. Handelt es sich bei einer juristischen Person, die eine freie und quelloffene Software veröffentlicht, um eine gemeinnützige Organisation, die „so angelegt ist, dass sichergestellt ist, dass alle Einnahmen nach Abzug der Kosten zur Verwirklichung gemeinnütziger Ziele verwendet werden“ (Erwägungsgrund 18 der Cyberresilienzverordnung), gilt die von ihr veröffentlichte freie und quelloffene Software nicht als in den Verkehr gebracht. Wenn diese juristische Person der Definition des Begriffs „Verwalter“ entspricht, unterliegt sie den entsprechenden Pflichten (Artikel 24 der Cyberresilienzverordnung).

Beispiel 24: Eine juristische Person veröffentlicht einen kostenlosen und quelloffenen Browser, der direkt über Suchmaschinenpartnerschaften monetarisiert wird, dessen gesamte Einnahmen nach Abzug der Kosten jedoch für gemeinnützige Ziele verwendet werden. Der Browser gilt nicht als im Sinne der Cyberresilienzverordnung in den Verkehr gebracht. Die juristische Person, die ihn veröffentlicht, unterliegt den für Verwalter geltenden Pflichten.

3.2.7. *Integration durch andere Hersteller*

67. In einigen Fällen wird eine freie und quelloffene Software von einer eindeutig identifizierbaren natürlichen oder juristischen Person veröffentlicht, doch die Software ist „zur Integration durch andere Hersteller in ihre eigenen Produkte mit digitalen Elementen bestimmt“. In solchen Fällen gilt die freie und quelloffene Software nicht als in der EU in den Verkehr gebracht, es sei denn, sie wird von der Person, die sie veröffentlicht (d. h. dem ursprünglichen Hersteller), im Einklang mit den vorherigen Abschnitten dieser Leitlinien zusätzlich auch monetarisiert.

68. Wird diese freie und quelloffene Software nicht in den Verkehr gebracht, so würde die juristische Person, die sie veröffentlicht, den Pflichten von Verwaltern unterliegen, wenn sie im Einklang mit der Definition des Begriffs „Verwalter“ nachhaltig Unterstützung leistet.

Beispiel 25: Eine juristische Person veröffentlicht eine Bibliothek für den Aufbau von Benutzeroberflächen in Form freier und quelloffener Software. Sie monetarisiert die Bereitstellung dieser Bibliothek nicht, sondern integriert sie in eines ihrer Produkte mit digitalen Elementen (das wiederum in den Verkehr gebracht wird). Die Bibliothek gilt nicht als im Sinne der Cyberresilienzverordnung in den Verkehr gebracht, sondern ist für die Integration in Produkte mit digitalen Elementen bestimmt. Die juristische Person, die sie veröffentlicht, ist ihr Verwalter.

Beispiel 26: Eine juristische Person bringt ein Betriebssystem in den Verkehr und veröffentlicht auch Bibliotheken freier und quelloffener Software, die Nutzern dieses Betriebssystems als Referenzimplementierungen dienen. Die juristische Person monetarisiert diese Bibliotheken, die für die Integration in andere Produkte mit digitalen Elementen bestimmt sind, nicht. Folglich ist die juristische Person, die diese Bibliotheken freier und quelloffener Software veröffentlicht, deren Verwalter.

3.3. **Verwalter quelloffener Software**

69. Mit der Cyberresilienzverordnung wird angesichts „der Bedeutung für die Cybersicherheit, die vielen Produkten mit digitalen Elementen zukommt, die als freie und quelloffene Software eingestuft sind und im Sinne dieser Verordnung veröffentlicht, aber nicht auf dem Markt bereitgestellt werden“ (Erwägungsgrund 19 der Cyberresilienzverordnung) die neue rechtliche Kategorie „Verwalter quelloffener Software“ eingeführt.

70. In einigen Fällen wird eine freie und quelloffene Software veröffentlicht, aber im Sinne der Cyberresilienzverordnung nicht von einer juristischen Person in den Verkehr gebracht, „die den Zweck oder das Ziel hat, die Entwicklung [freier und quelloffener Software, die] … für kommerzielle Tätigkeiten bestimmt [ist], systematisch und nachhaltig zu unterstützen, und die die Brauchbarkeit dieser Produkte sicherstellt“ (Artikel 3 Nummer 14 der Cyberresilienzverordnung). In solchen Fällen unterliegt diese juristische Person den Pflichten von Verwaltern.

71. Ein Verwalter ist als „eine juristische Person, bei der es sich nicht um einen Hersteller handelt“ definiert, da ein Hersteller definitionsgemäß die natürliche oder juristische Person ist, die Produkte mit digitalen Elementen unter ihrem eigenen Namen oder ihrer eigenen Marke in den Verkehr bringt („vermarktet“). Eine juristische Person kann nur Verwalter von Produkten mit digitalen Elementen sein, die als freie und quelloffene Software gelten und die zwar veröffentlicht, aber im Sinne der Cyberresilienzverordnung nicht auf dem Markt bereitgestellt werden. Der Begriff des „Verwalters“ ist daher auf bestimmte Fälle von freier und quelloffener Software anwendbar, die „letztlich für kommerzielle Tätigkeiten wie die Integration in kommerzielle Dienste oder kostenpflichtige Produkte mit digitalen Elementen bestimmt sind“ (Erwägungsgrund 19 der Cyberresilienzverordnung ([13])), im Sinne der Cyberresilienzverordnung aber nicht auf dem Markt bereitgestellt werden, und für die die juristische Person, welche die betreffende freie und quelloffene Software veröffentlicht, eine systematische Unterstützung sicherstellt.

72. Die Tatsache, ein Verwalter einer bestimmten freien und quelloffenen Software zu sein, bedeutet nicht, dass diese juristische Person zwangsläufig auch Verwalter anderer von ihr veröffentlichter freier und quelloffener Software ist. Ebenso bedeutet die Tatsache, Hersteller einer bestimmten freien und quelloffenen Software zu sein, nicht, dass diese juristische Person nicht auch ein Verwalter anderer freier und quelloffener Software sein kann. Dazu gehört auch die Bereitstellung von „Community-Versionen“ derselben freien und quelloffenen Software, wie in Abschnitt *3.2.1 Erheben eines Entgelts* beschrieben.

73. Eine juristische Person kann folglich gleichzeitig ein Verwalter einer bestimmten freien und quelloffenen Software (für welche der Verwalter systematisch und nachhaltig Unterstützung leistet und deren Brauchbarkeit er sicherstellt) und ein Hersteller einer anderen bestimmten freien und quelloffenen Software (die er in den Verkehr bringt) sein. Mit anderen Worten kann es sein, dass ein und dieselbe juristische Person für verschiedene Projekte in Bezug auf freie und quelloffene Software unterschiedliche Rollen zu erfüllen hat.

74. Diese juristische Person muss für jede von ihr veröffentlichte bestimmte freie und quelloffene Software prüfen, ob sie als im Sinne der Cyberresilienzverordnung in den Verkehr gebracht gilt. Ist dies der Fall, wird dieser Rechtsträger zum Hersteller der Software. Wenn die freie und quelloffene Software nicht als in den Verkehr gebracht gilt, kann die juristische Person ihr Verwalter sein, wenn die Software für kommerzielle Tätigkeiten bestimmt ist und die juristische Person sie im Einklang mit der Definition des Begriffs „Verwalter“ nachhaltig unterstützt ([14]).

3.3.1. *Dauerhafte Unterstützung und Gewährleistung der Brauchbarkeit freier und quelloffener Software*

75. In Erwägungsgrund 19 wird erläutert, dass die dauerhafte Unterstützung der Entwicklung eines Produkts mit digitalen Elementen Folgendes umfassen kann (ohne darauf beschränkt zu sein): i) das Hosting und die Verwaltung von Plattformen für die Zusammenarbeit bei der Softwareentwicklung; ii) das Hosting von Quellcode oder Software; iii) das Verwalten oder Administrieren von Produkten mit digitalen Elementen, die als freie und quelloffene Software eingestuft sind, sowie iv) die Steuerung der Entwicklung solcher Produkte.

76. Dies kann beispielsweise bei einem Rechtsträger der Fall sein, der freie und quelloffene Software zur Integration in seine eigenen Produkte mit digitalen Elementen entwickelt und sie dann veröffentlicht, ohne sie in den Verkehr zu bringen. Dies wird auch in Abschnitt *3.2.7 Integration durch andere Hersteller* erörtert. In diesem Fall ist der Rechtsträger kein Hersteller der Software, kann aber ihr Verwalter sein. Darüber hinaus gilt, wie auch in den vorstehenden Abschnitten erläutert, ein Rechtsträger, der eine kostenlose Version (oder Community-Version) und eine monetarisierte Version derselben freien und quelloffenen Software veröffentlicht, als ein Verwalter der kostenlosen Version (oder Community-Version) und als ein Hersteller der monetarisierten Version.

77. Ebenso ist ein Rechtsträger, der eine freie und quelloffene Software monetarisiert, aber ein gemeinnütziger Rechtsträger ist, dessen Einnahmen nach Kosten für das Erreichen nicht gewinnorientierter Ziele verwendet werden (weshalb seine freie und quelloffene Software im Sinne der Cyberresilienzverordnung nicht in den Verkehr gebracht wird, wie in Abschnitt *3.2.6 Zum Erreichen gemeinnütziger Ziele* erörtert), ein Verwalter der von ihm veröffentlichten freien und quelloffenen Software.

78. Darüber hinaus bieten bestimmte Stiftungen Kooperationsplattformen mit verschiedenen Formen der Governance an, die es Herstellern ermöglichen, regelmäßig zur Entwicklung von freier und quelloffener Software beizutragen, und/oder regelmäßig von Herstellern finanziert werden. Solche Stiftungen sind in Bezug auf bestimmte freie und quelloffene Software, die für kommerzielle Tätigkeiten bestimmt ist und für die die Stiftung dauerhafte Unterstützung bietet, als Verwalter zu betrachten. Wie in Abschnitt *3.3 Verwalter quelloffener Software* erläutert, unterliegt eine solche Stiftung womöglich jedoch nicht den Pflichten im Rahmen der Cyberresilienzverordnung für andere spezifische freie und quelloffene Software, die sie hostet, wenn sie keine systematische Unterstützung für eine bestimmte freie und quelloffene Software leistet, ihre Brauchbarkeit nicht sicherstellt und/oder wenn diese konkrete Software nicht für kommerzielle Tätigkeiten bestimmt ist.

([13]) Dieser Begriff ist auch in der Formulierung „für kommerzielle Tätigkeiten bestimmt“ enthalten, die in der Definition des Begriffs „Verwalter quelloffener Software“ in Artikel 3 Nummer 14 der Cyberresilienzverordnung verwendet wird.

([14]) Es ist möglich, dass die juristische Person auch keinen Pflichten im Rahmen der Cyberresilienzverordnung unterliegt, wenn: i) eine bestimmte freie und quelloffene Software im Sinne der Cyberresilienzverordnung nicht als in den Verkehr gebracht gilt und ii) die juristische Person in Bezug auf diese freie und quelloffene Software nicht der Definition des Begriffs „Verwalter“ entspricht.

79. Die Art der „dauerhaften Unterstützung“, die Stiftungen und ähnliche Organisationen für bestimmte Projekte im Bereich freier und quelloffener Software leisten, kann sehr unterschiedlich sein. Beispielsweise bieten bestimmte Rechtsträger nur nichttechnische Unterstützung an, etwa die Verwaltung des Branding von Projekten, die Festlegung von Governance-Regeln, die Organisation von Veranstaltungen der Gemeinschaft oder die Sammlung von Spenden. Andere Rechtsträger stellen auch die zugrunde liegende IT-Infrastruktur bereit, die für die Durchführung des Projekts erforderlich ist, und übernehmen beispielsweise das Hosting von Quellcode-Sammlungen, stellen Versionskontrollsysteme bereit oder generieren Signaturschlüssel. Andere gehen in der Art der von ihnen geleisteten Unterstützung noch weiter und stellen aktiv technische Ressourcen für das Projekt bereit, beispielsweise durch die Beschäftigung von Entwicklern, die Koordinierung von Entwicklungsarbeiten, die Überprüfung oder Zusammenführung von Code, die Versionsverwaltung oder die Bearbeitung von Schwachstellenmeldungen und Sicherheits-Patches. Während alle Rechtsträger, die nach der Cyberresilienzverordnung als Verwalter gelten, die Pflichten nach Artikel 24 Absätze 1 und 2 erfüllen müssen, ist das Ausmaß, in dem die in Artikel 14 Absätze 1, 3 und 8 festgelegten Pflichten für diese Rechtsträger gelten, gemäß Artikel 24 Absatz 3 je nach Art der von ihnen geleisteten Unterstützung unterschiedlich.

80. Beispielsweise ist ein Verwalter, der nur nichttechnische Unterstützung leistet, per definitionem nicht an der Entwicklung des Produkts mit digitalen Elementen beteiligt und daher auch nicht verpflichtet, aktiv ausgenutzte Schwachstellen zu melden. Dieser Verwalter stellt auch keine Netz- und Informationssysteme für die Entwicklung solcher Produkte mit digitalen Elementen bereit und ist daher nicht verpflichtet, schwerwiegende Sicherheitsvorfälle der ENISA und den CSIRTs oder den betroffenen Nutzern zu melden. Erlangt der Verwalter jedoch Kenntnis von einer aktiv ausgenutzten Schwachstelle (beispielsweise durch einen Bericht von externen Quellen wie Forschern im Bereich der Informationssicherheit), sollte er die Informationen im Einklang mit seiner Cybersicherheitsstrategie an die Wartungsbetriebe des Produkts mit digitalen Elementen weiterleiten. Die Wartungsbetriebe der Produkte mit digitalen Elementen und/oder die Verwalter sollten auch in Erwägung ziehen, die Schwachstelle auf freiwilliger Basis gemäß Artikel 15 zu melden.

81. Stellt ein Verwalter hingegen die zugrunde liegende IT-Infrastruktur für bestimmte Produkte mit digitalen Elementen bereit, so ist er verpflichtet, die ENISA und die CSIRTs gemäß Artikel 14 Absatz 3 über alle schwerwiegenden Sicherheitsvorfälle im Zusammenhang mit dieser Infrastruktur zu unterrichten, die sich auf die Sicherheit von Produkten mit digitalen Elementen auswirken. Er ist gegebenenfalls auch verpflichtet, alle Nutzer zu informieren (beispielsweise durch eine allgemeine Bekanntmachung). Wie im vorstehenden Punkt dargelegt, ist der Verwalter zwar nicht verpflichtet, aktiv ausgenutzte Schwachstellen, von denen er Kenntnis erlangt, zu melden, doch sollte er den sachgerechten Umgang mit Schwachstellen fördern und eine freiwillige Meldung gemäß Artikel 15 in Erwägung ziehen.

82. Schließlich muss ein Verwalter, der auch technische Ressourcen für bestimmte Produkte mit digitalen Elementen bereitstellt, i) gemäß Artikel 14 Absatz 1 aktiv ausgenutzte Schwachstellen, von denen er Kenntnis erlangt, melden und ii) gegebenenfalls alle Nutzer informieren. Sofern der Verwalter auch in direkter Beziehung zu betroffenen Nutzern steht, ist er auch verpflichtet, diese gemäß Artikel 14 Absatz 8 direkt zu informieren.

83. Stellt ein Rechtsträger die systematische und dauerhafte Unterstützung für eine bestimmte freie und quelloffene Software ein, erfüllt er möglicherweise nicht mehr die Definition des Begriffs „Verwalter“ und unterliegt daher möglicherweise nicht mehr den entsprechenden Pflichten. In solchen Fällen ist dieser Rechtsträger aufgefordert, die Änderung seines Status in Bezug auf diese konkrete freie und quelloffene Software klar mitzuteilen.

84. In bestimmten Situationen kann ein Rechtsträger, der Verwalter eines bestimmten Projekts war, beschließen, dieses Projekt direkt zu monetarisieren, wodurch das Produkt mit digitalen Elementen in den Verkehr gebracht wird und der Hersteller den Pflichten im Rahmen der Cyberresilienzverordnung unterliegt. Unter diesen Umständen gilt dieser Rechtsträger ab dem Zeitpunkt, zu dem er das Produkt mit digitalen Elementen in den Verkehr bringt, als Hersteller des Produkts mit digitalen Elementen (jedoch nicht in Bezug auf frühere Versionen, für die er als Verwalter tätig war).

3.4. **„Contributor“ und nachgelagerte Verwendungszwecke**

85. Wie bereits in Abschnitt *3.1 Feststellen, ob freie und quelloffene Software in die eigene Verantwortung fällt* erwähnt, ist in der Cyberresilienzverordnung klar festgelegt, dass sie „nicht für natürliche oder juristische Personen [gilt], die mit Quellcode zu Produkten mit digitalen Elementen beitragen, die als freie und quelloffene Software eingestuft sind und nicht ihrer Verantwortung unterliegen“ (Erwägungsgrund 18).

86. Hersteller von Produkten mit digitalen Elementen, die Komponenten freier und quelloffener Software in ihre eigenen Produkte mit digitalen Elementen integrieren, übernehmen auch keine Verantwortung dafür, dass jede einzelne dieser Komponenten der Cyberresilienzverordnung entspricht, selbst wenn die Hersteller Quellcode zu ihrer Wartung beitragen.

87. Ebenso hat die bloße Tatsache, dass Hersteller Komponenten freier und quelloffener Software in ihre eigenen (monetarisierten) Produkte mit digitalen Elementen integrieren, keine Auswirkungen auf den Status der betreffenden Komponente freier und quelloffener Software im Rahmen der Cyberresilienzverordnung. Wartungsbetriebe von Komponenten freier und quelloffener Software, die nicht in den Verkehr gebracht werden, haben keine Verpflichtungen gegenüber anderen Rechtsträgern, die solche Komponenten möglicherweise in ihre Produkte mit digitalen Elementen integrieren. Ob die Cyberresilienzverordnung für eine bestimmte Komponente freier und quelloffener Software gilt, hängt allein davon ab, ob die natürliche oder juristische Person, die sie veröffentlicht, sie in den Verkehr bringt.

88. Dennoch müssen Hersteller von Produkten mit digitalen Elementen, die Komponenten freier und quelloffener Software enthalten, hinsichtlich ihrer eigenen Produkte mit digitalen Elementen die Cyberresilienzverordnung einhalten. Sie haben auch eine Sorgfaltspflicht gemäß Artikel 13 Absatz 5 in Bezug auf die Komponenten freier und quelloffener Software, die sie in ihre eigenen Produkte integrieren. Darüber hinaus sind sie verpflichtet, Schwachstellen in integrierten Komponenten zu melden und Sicherheits-Patches gemäß Artikel 13 Absatz 6 weiterzugeben. Näheres zu diesem Thema ist Abschnitt *9.2.1 Vorgelagerte Meldung und gemeinsame Nutzung von Sicherheits-Patches* zu entnehmen.

3.5. **Veranschaulichende Szenarien**

89. Die folgenden Beispiele sind rein hypothetisch und dienen nur der Veranschaulichung der verschiedenen in den vorstehenden Abschnitten erläuterten Sachverhalte.

Beispiel 27: Einzelentwickler A hat eine freie und quelloffene Software entwickelt. Entwickler A veröffentlicht diese freie und quelloffene Software unter seinem eigenen Namen oder seiner eigenen Marke, verlangt jedoch für ihre Nutzung kein Entgelt. Die Software wird offen geteilt und ist frei zugänglich, sodass alle auf sie zugreifen, sie nutzen, ändern und weiterverbreiten können. Zudem hat Entwickler A in die Software einen Link zu einer Plattform integriert, über die freiwillige Spenden gesammelt werden.

Die Unternehmen B, C und D integrieren diese freie und quelloffene Software in ihre eigenen Produkte mit digitalen Elementen. Zur Unterstützung der laufenden Wartung der Software leisten die Unternehmen B, C und D freiwillige Spenden an Entwickler A. Diese Spenden ermöglichen es Entwickler A, das Projekt aktiv zu pflegen.

Diese freie und quelloffene Software wird im Sinne der Cyberresilienzverordnung nicht in den Verkehr gebracht. Entwickler A hat keine Pflichten im Rahmen der Cyberresilienzverordnung. Die Unternehmen B, C und D müssen bei der Integration dieser freien und quelloffenen Software in ihre eigenen Produkte mit digitalen Elementen ihre Sorgfaltspflicht gemäß Artikel 13 Absatz 5 erfüllen.

Beispiel 28: Die gemeinnützige Stiftung F veröffentlicht eine Komponente freier und quelloffener Software für die Integration in andere, kommerzielle Produkte mit digitalen Elementen. Die Stiftung F verpflichtet sich, diese freie und quelloffene Software dauerhaft zu unterstützen, um ihre Brauchbarkeit und Akzeptanz zu gewährleisten. Die Unternehmen A, B und C integrieren diese freie und quelloffene Software in ihre eigenen Produkte mit digitalen Elementen. Die Unternehmen A und B tragen freiwillig durch einen Teil der Arbeitszeit ihrer eigenen Entwickler zur Entwicklung und Pflege von Projekten im Rahmen freier und quelloffener Software innerhalb der Stiftung F bei, darunter auch für diese freie und quelloffene Software.

Da die Stiftung F ein gemeinnütziger Rechtsträger ist, der so organisiert ist, dass seine Einnahmen nach Kosten zur Erreichung gemeinnütziger Ziele verwendet werden, gilt die freie und quelloffene Software im Sinne der Cyberresilienzverordnung nicht als in den Verkehr gebracht. Die Stiftung F ist der Verwalter der freien und quelloffenen Software und unterliegt den entsprechenden Pflichten gemäß Artikel 24. Die Unternehmen A, B und C müssen bei der Integration dieser freien und quelloffenen Software in ihre eigenen Produkte mit digitalen Elementen ihre Sorgfaltspflicht gemäß Artikel 13 Absatz 5 erfüllen.

Beispiel 29: Unternehmen A hat eine Komponente freier und quelloffener Software für die Integration in seine eigenen Produkte mit digitalen Elementen entwickelt. Außerdem veröffentlicht es diese freie und quelloffene Software separat unter seinem eigenen Namen oder seiner eigenen Marke und pflegt sie aktiv. Es verlangt jedoch weder ein Entgelt für ihre Nutzung noch nutzt es eine andere Form der Monetarisierung. Die Unternehmen B, C und D integrieren diese freie und quelloffene Software in ihre eigenen Produkte mit digitalen Elementen und tragen freiwillig mit einem Teil der Arbeitszeit ihrer Entwickler zur Wartung dieser Software bei.

Diese freie und quelloffene Software gilt im Sinne der Cyberresilienzverordnung als nicht in den Verkehr gebracht. Das Unternehmen A ist nicht ihr Hersteller, sondern ihr Verwalter. Die Unternehmen B, C und D müssen bei der Integration dieser freien und quelloffenen Software in ihre eigenen Produkte mit digitalen Elementen ihre Sorgfaltspflicht gemäß Artikel 13 Absatz 5 erfüllen.

Beispiel 30: Unternehmen A veröffentlicht eine freie und quelloffene Software unter seinem eigenen Namen oder seiner eigenen Marke und bietet sie als kostenpflichtige Version an, die bestimmte Vorteile wie technische Hilfe oder Leistungsoptimierung umfasst. Entwickler der Unternehmen B, C und D tragen zur Wartung der freien und quelloffenen Software bei, die jedoch weiterhin unter der Kontrolle von Unternehmen A bleibt.

Unternehmen A gilt als Hersteller dieser freien und quelloffenen Software ([15]). Die Unternehmen B, C und D unterliegen für diese konkrete freie und quelloffene Software keinen Pflichten im Rahmen der Cyberresilienzverordnung. Wenn sie diese freie und quelloffene Software in ihre eigenen Produkte mit digitalen Elementen integrieren, sind sie verpflichtet, ihre Sorgfaltspflicht gemäß Artikel 13 Absatz 5 erfüllen.

Beispiel 31: Unternehmen A veröffentlicht eine freie und quelloffene Software unter seinem eigenen Namen oder seiner eigenen Marke und sorgt für ihre laufende Wartung, um ihre langfristige Brauchbarkeit zu gewährleisten, damit diese Software in die Produkte anderer Unternehmen mit digitalen Elementen integriert werden kann. Unternehmen A verlangt kein Entgelt für die Nutzung der Software, verarbeitet keine personenbezogenen Daten, die es über das Produkt mit digitalen Elementen erhebt, und verkauft auch keine Unterstützungsdienste im Zusammenhang mit der Veröffentlichung der freien und quelloffenen Software.

Unternehmen B trägt Code und Arbeitszeit seiner eigenen Entwickler zur Wartung der freien und quelloffenen Software bei, vertreibt diese jedoch nicht kommerziell. Unternehmen B bietet unabhängig vom Vertrieb der freien und quelloffenen Software technische Unterstützungsdienste an. Unternehmen A gilt als Verwalter dieser freien und quelloffenen Software, während Unternehmen B im Rahmen der Cyberresilienzverordnung im Zusammenhang mit dieser Software keine Pflichten hat.

Beispiel 32: Ein gemeinnütziger Rechtsträger, der so organisiert ist, dass alle Einnahmen nach Abzug der Kosten zur Erreichung gemeinnütziger Ziele verwendet werden, veröffentlicht eine Komponente freier und quelloffener Software. Das Unternehmen leistet dauerhafte Unterstützung, um die langfristige Brauchbarkeit des Projekts zu gewährleisten. Die Wartung wird aus öffentlichen Mitteln, beispielsweise Forschungszuschüssen, finanziert. Zusätzliche Entwicklungen, einschließlich neuer Funktionen, werden durch Spenden und spezifische Projekte finanziert, die in Partnerschaft mit Herstellern durchgeführt werden, die diese freie und quelloffene Software in ihre Produkte mit digitalen Elementen integrieren. Diese Funktionen werden in die Codebasis der freien und quelloffenen Software aufgenommen.

Der gemeinnützige Rechtsträger, der die freie und quelloffene Software veröffentlicht, gilt als Verwalter dieser Komponente freier und quelloffener Software. Ein Hersteller, der zur Entwicklung bestimmter Funktionen beigetragen hat, wird nicht zum Hersteller dieser Komponente freier und quelloffener Software. Integriert der Hersteller die freie und quelloffene Software in sein eigenes Produkt mit digitalen Elementen, muss er seiner Sorgfaltspflicht gemäß Artikel 13 Absatz 5 genügen.

Beispiel 33: Ein gemeinnütziger Rechtsträger, der so organisiert ist, dass nach Abzug der Kosten alle Gewinne zur Erreichung gemeinnütziger Ziele verwendet werden, veröffentlicht ein Softwareentwicklungspaket (Software Development Kit, SDK) für freie und quelloffene Software und sorgt für dessen laufende Wartung. Das Softwareentwicklungspaket wird offen geteilt und steht für den Zugang, die Nutzung, die Änderung und die Weiterverteilung zur allgemeinen freien Verfügung. Die Finanzierung erfolgt durch Mitgliedsbeiträge, die an den gemeinnützigen Rechtsträger gezahlt werden, und von Mitgliedsorganisationen beschäftigte Entwickler tragen mit Code und anderen Ressourcen zur Entwicklung des Softwareentwicklungspakets bei. Die Hersteller verwenden das Softwareentwicklungspaket als Komponente für die Herstellung anderer Produkte mit digitalen Elementen.

Der gemeinnützige Rechtsträger, der dieses Softwareentwicklungspaket veröffentlicht, ist dessen Verwalter. Die Mitglieder der Stiftung sind nicht dafür verantwortlich, dass das Softwareentwicklungspaket den Bedingungen der Cyberresilienzverordnung entspricht. Verwenden Hersteller das Softwareentwicklungspaket für die Herstellung ihres eigenen Produkts mit digitalen Elementen, müssen sie ihrer Sorgfaltspflicht gemäß Artikel 13 Absatz 5 genügen.

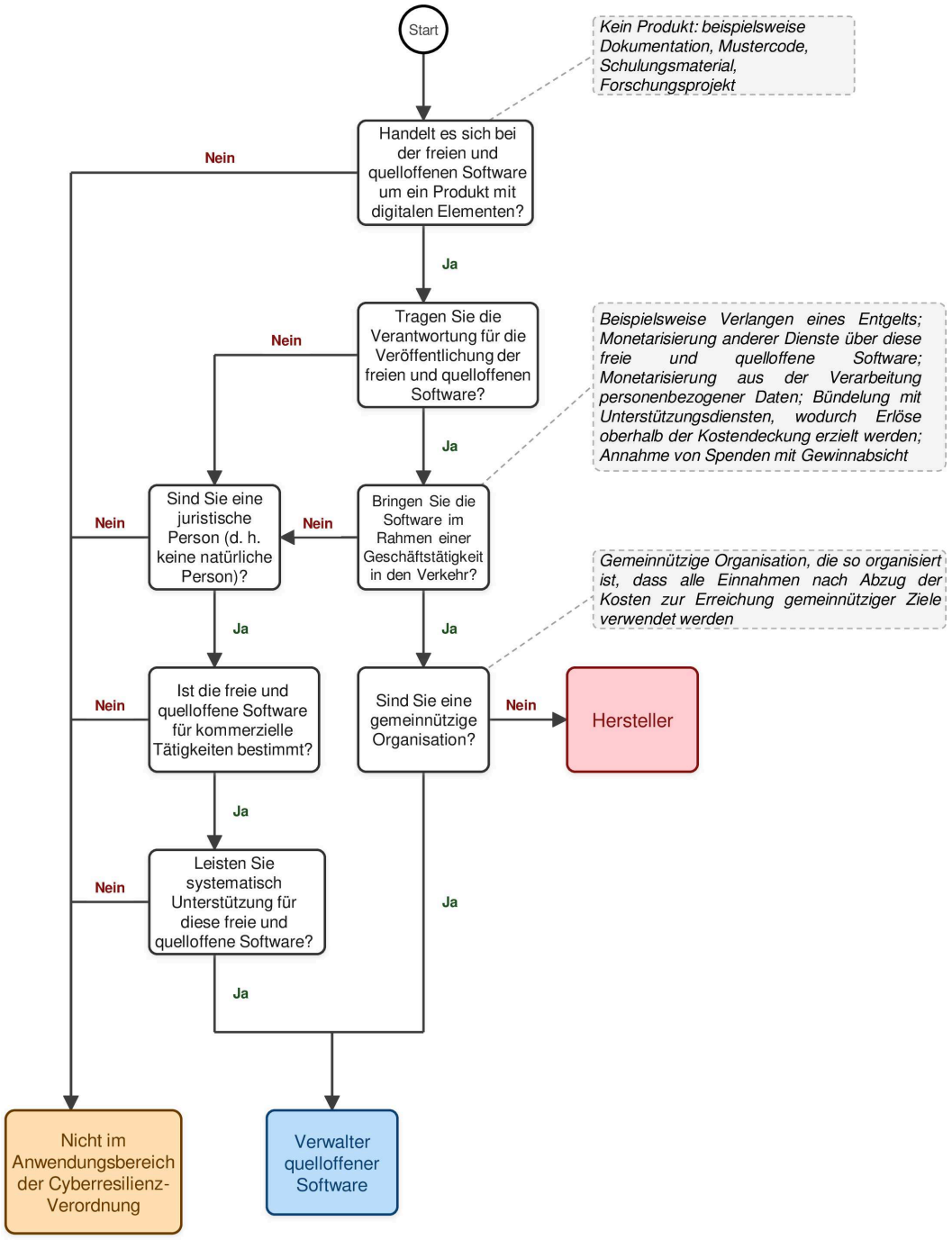
Beispiel 34: Ein einzelner Entwickler veröffentlicht eine Bibliothek freier und quelloffener Software in einem öffentlichen Paket-Repository für eine bestimmte Programmiersprache und pflegt sie aktiv. In der Dokumentation zum Paket fügt der Entwickler einen Link zum Sammeln von Spenden hinzu. Ein Hersteller lädt diese Bibliothek kostenlos aus dem Repository herunter und integriert sie in sein eigenes Produkt mit digitalen Elementen.

Der einzelne Entwickler und das Paket-Repository haben keine Pflichten im Rahmen der Cyberresilienzverordnung. Der Hersteller, der die Bibliothek integriert, muss seiner Sorgfaltspflicht gemäß Artikel 13 Absatz 5 genügen.

([15]) Es sei denn, Unternehmen A ist ein gemeinnütziger Rechtsträger, der so organisiert ist, dass alle Gewinne nach Kosten zur Erreichung gemeinnütziger Ziele verwendet werden; in diesem Fall wäre es der Verwalter dieser freien und quelloffenen Software.

Abbildung 1

Stilisiertes Flussdiagramm zur Anwendbarkeit der Cyberresilienzverordnung auf freie und quelloffene Software



4. WESENTLICHE ÄNDERUNGEN UND ERSATZTEILE

90. In Artikel 3 Nummer 30 der Cyberresilienzverordnung ist eine „wesentliche Änderung“ definiert als eine Änderung des Produkts mit digitalen Elementen nach dessen Inverkehrbringen, die i) sich auf die Konformität des Produkts mit digitalen Elementen den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I auswirkt oder ii) oder zu einer Änderung des bestimmungsgemäßen Zwecks, für den das Produkt mit digitalen Elementen bewertet wurde, führt.

91. Der Begriff der wesentlichen Änderung ist für die Feststellung der im Rahmen der Cyberresilienzverordnung in einer Reihe von Fällen bestehenden Pflichten relevant, darunter auch in den folgenden Fällen:

a) Gemäß Artikel 21 gilt ein Einführer oder Händler, der eine wesentliche Änderung an einem bereits in den Verkehr gebrachten Produkt mit digitalen Elementen vornimmt, als dessen Hersteller,

b) gemäß Artikel 22 gilt jede natürliche oder juristische Person, die eine wesentliche Änderung an einem Produkt mit digitalen Elementen vornimmt und dieses Produkt auf dem Markt bereitstellt, als dessen Hersteller,

c) gemäß Artikel 69 Absatz 2 gilt jede natürliche oder juristische Person, die nach dem 11. Dezember 2027 eine wesentliche Änderung an einem vor dem 11. Dezember 2027 in den Verkehr gebrachten Produkt mit digitalen Elementen vornimmt und dieses Produkt in den Verkehr bringt, als dessen Hersteller,

d) für Hersteller von Produkten mit digitalen Elementen, die nach dem 11. Dezember 2027 in den Verkehr gebracht werden, um festzustellen, ob ein Produkt mit digitalen Elementen aufgrund von Änderungen, die nach diesem Datum vorgenommen wurden, einem neuen Konformitätsbewertungsverfahren unterzogen werden muss, insbesondere angesichts des der Softwareentwicklung innewohnenden Wiederholungscharakters.

92. Daher ist es wichtig, den Wirtschaftsakteuren Leitlinien an die Hand zu geben, damit verständlicher wird, wann Hardware- oder Softwareänderungen als wesentliche Änderungen einzustufen sind.

4.1. **Physische Reparaturen**

93. In Erwägungsgrund 42 der Cyberresilienzverordnung heißt es: „Wird ein Produkt mit digitalen Elementen einer ‚Überholung' ‚Wartung' und ‚Reparatur' im Sinne des Artikels 2 Nummern 18, 19 und 20 der Verordnung (EU) 2024/1781 des Europäischen Parlaments und des Rates unterzogen, führt dies nicht unbedingt zu einer wesentlichen Änderung des Produkts, wenn beispielsweise die Zweckbestimmung und die Funktionen nicht geändert werden und das Risikoniveau gleich bleibt. Die Aufrüstung eines Produkts mit digitalen Elementen durch den Hersteller könnte jedoch zu Änderungen in der Konzeption und Entwicklung des Produkts führen und sich daher auf seine Zweckbestimmung und die Konformität mit den in dieser Verordnung festgelegten Anforderungen auswirken." Dies steht im Einklang mit Abschnitt 2.1 des „Blue Guide", in dem es heißt: „Ein Produkt, an dem nach seiner Inbetriebnahme wesentliche Änderungen oder Überarbeitungen vorgenommen wurden, kann als neues Produkt angesehen werden, wenn i) seine ursprüngliche Leistung, Verwendung oder Bauart geändert wurde, ohne dass dies bei der ursprünglichen Risikobewertung vorgesehen war, ii) sich die Art der Gefahr verändert oder das Risikoniveau im Vergleich zu den einschlägigen Harmonisierungsrechtsvorschriften der Union erhöht hat und iii) das Produkt zur Verfügung gestellt wird (oder in Betrieb genommen wird, wenn die Inbetriebnahme ebenfalls in den Anwendungsbereich der geltenden Rechtsvorschriften fällt). Dies ist von Fall zu Fall und insbesondere vor dem Hintergrund des Ziels der Rechtsvorschriften und der Art der Produkte im Anwendungsbereich der betreffenden Rechtsvorschrift zu entscheiden."

94. Überholungs-, Wartungs- oder Reparaturvorgänge, die zu physischen Änderungen von bereits in den Verkehr gebrachten Produkten mit digitalen Elementen führen, stellen nicht notwendigerweise wesentliche Änderungen dar. Daher sollte eine Einzelfallbewertung durchgeführt werden, um festzustellen, ob sich eine solche physische Änderung auf die Konformität des Produkts mit den grundlegenden Anforderungen in Anhang I Teil I auswirkt oder zu einer Änderung der Zweckbestimmung des Produkts führt, die Gegenstand der Bewertung der Cybersicherheitsrisiken ist.

95. Das Ersetzen von fehlerhaften Teilen oder Verschleißartikeln durch Teile mit besserer Leistung (beispielsweise aufgrund des technischen Fortschritts oder weil das alte Teil nicht mehr hergestellt wird) führt nicht per se zu einer wesentlichen Änderung des reparierten Produkts mit digitalen Elementen. Zu einer solchen Änderung kommt es nur, wenn sich die Leistung oder die Funktionsweise des reparierten Produkts mit digitalen Elementen i) auf seine Konformität mit den grundlegenden Anforderungen auswirkt oder ii) zu einer Änderung der Zweckbestimmung führt, die durch die Risikobewertung nicht abgedeckt wurde.

Beispiel 35: Der Hersteller eines Computerservers führt eine Reparatur durch, indem er einen defekten RAM durch einen neuen, leistungsfähigeren Speicher ersetzt. Der Server entspricht danach weiterhin den grundlegenden Anforderungen. Der Server ist leistungsstärker, aber seine neue Leistung liegt nach wie vor im Rahmen der beabsichtigten Verwendung des Servers, wie sie bei der Bewertung der Cybersicherheitsrisiken berücksichtigt wurde. Der Computerserver gilt nicht als wesentlich geändert.

4.2. **Ersatzteile**

96. Nach Artikel 2 Absatz 6 der Cyberresilienzverordnung unterliegen Ersatzteile, die dazu bestimmt sind, identische Komponenten zu ersetzen, und die nach denselben Spezifikationen hergestellt werden wie diese Komponenten, nicht der Cyberresilienzverordnung. In Erwägungsgrund 29 heißt es ferner, dass die Ausnahme sowohl für Ersatzteile für Produkte mit digitalen Elementen gilt, die vor dem Inkrafttreten der Cyberresilienzverordnung bereitgestellt wurden, als auch für Ersatzteile, die bereits einem Konformitätsbewertungsverfahren gemäß der Verordnung unterzogen wurden.

97. Die Ausnahme gemäß Artikel 2 Absatz 6 der Cyberresilienzverordnung sollte so verstanden werden, dass sie nur dann gilt, wenn das Ersatzteil speziell zur Reparatur oder zur Verlängerung der Haltbarkeit eines bereits in den Verkehr gebrachten Produkts mit digitalen Elementen (vor oder nach dem 11. Dezember 2027) geliefert wird. Wird ein Produkt mit digitalen Elementen als eigenständiges Produkt bereitgestellt, ohne dass es mit der Wartung oder Reparatur eines bereits existierenden Produkts mit digitalen Elementen in Verbindung steht, so wird es im Sinne der Cyberresilienzverordnung in den Verkehr gebracht und sollte nicht als Ersatzteil betrachtet werden, das in den Anwendungsbereich des Artikels 2 Absatz 6 fällt. Der Wartungs- oder Reparaturzweck sollte aus dem Kontext der Bereitstellung hervorgehen, beispielsweise durch Identifizierung des Produkts mit digitalen Elementen oder der Produktfamilie im Auftrag oder im kommerziellen Angebot oder durch Bereitstellung über Kundendienst- oder Servicekanäle. Entsprechende Nachweise sollten auch den Marktüberwachungsbehörden zur Verfügung gestellt werden. Der Umstand, dass ein Produkt mit digitalen Elementen technisch dazu verwendet werden könnte, ein Bauteil zu ersetzen, reicht für sich genommen nicht aus, um die Ausnahmebestimmung auf dieses Produkt anwenden zu können, wenn solche Elemente fehlen.

98. Wenn also ein Ersatzteil mit einer Komponente identisch ist, die bereits in einem Produkt mit digitalen Elementen enthalten ist, das entweder vor dem Inkrafttreten der Cyberresilienzverordnung in den Verkehr gebracht wurde oder das im Einklang mit der Cyberresilienzverordnung in den Verkehr gebracht wurde, unterliegt dieses Ersatzteil nicht der Cyberresilienzverordnung.

99. Bei der Bewertung, ob ein Ersatzteil als mit einer Komponente identisch angesehen werden sollte, sollte der Schwerpunkt auf dessen funktionalen Rolle in dem Produkt mit digitalen Elementen und den Merkmalen liegen, die für die Cybersicherheit relevant sein können. Auch wenn stets eine Einzelfallbewertung erforderlich ist, schließen Unterschiede, die sich nicht auf die Sicherheitsmerkmale oder das Cybersicherheitsrisikoprofil der Komponente auswirken, für sich genommen nicht aus, dass dieses Ersatzteil in den Anwendungsbereich von Artikel 2 Absatz 6 der Cyberresilienzverordnung fällt.

100. Unterschiede in den für die Cybersicherheit der Komponente relevanten Merkmalen wie etwa Algorithmen, Protokollen, kryptografischen Mechanismen, Zugangskontrollfunktionen oder anderen sicherheitsrelevanten Merkmalen können hingegen dazu führen, dass das neue Teil nicht als identisch mit der Komponente angesehen werden kann, die es ersetzen soll.

101. Wenn ein Ersatzteil nicht mit der Originalkomponente identisch ist, stellt dieses Ersatzteil ein eigenständiges Produkt mit digitalen Elementen dar und unterliegt daher der Cyberresilienzverordnung. In solchen Fällen ist zu beurteilen, ob im Hinblick auf die Zweckbestimmung der Ersatzkomponente die grundlegenden Anforderungen erfüllt sind. Von besonderer Bedeutung ist dabei die Funktion der Ersatzkomponente dahin gehend, die Kompatibilität oder Interoperabilität mit einem bestehenden Produkt mit digitalen Elementen sicherzustellen, und zwar auch, wenn es sich bei diesem Produkt um ein Produkt mit digitalen Elementen handelt, das vor dem Inkrafttreten der Cyberresilienzverordnung in den Verkehr gebracht wurde. Sind bestimmte grundlegende Anforderungen aufgrund dieser Zweckbestimmung oder technischer Beschränkungen nach vernünftigem Ermessen nicht erfüllbar, so muss der Hersteller dies in der Bewertung der Cybersicherheitsrisiken berücksichtigen und geeignete alternative Maßnahmen oder Ausgleichsmaßnahmen zur Risikominderung ergreifen, damit die Sicherheit des Produkts mit digitalen Elementen nicht beeinträchtigt ist. Wie auch in Abschnitt *2.6 Komplexe Systeme* erläutert, sind für eine transparente Beschreibung der erkannten Einschränkungen, der damit verbundenen Cybersicherheitsrisiken und der umgesetzten Risikominderungsmaßnahmen sowohl die technische Dokumentation als auch die Informationen und die Gebrauchsanleitung für den Nutzer ausschlaggebend. Wie in Abschnitt *4.1 Physische Reparaturen* erläutert, führt das bloße Ersetzen von fehlerhaften Teilen oder Verschleißartikeln durch Teile mit besserer Leistung nicht zu einer wesentlichen Änderung des reparierten Produkts mit digitalen Elementen.

Beispiel 36: Ein Hersteller bringt vernetzte Controller auf dem Unionsmarkt in den Verkehr. Bei einem der Controller erfolgt das Inverkehrbringen im Jahr 2026, vor dem Inkrafttreten der Cyberresilienzverordnung. In einem anderen Fall wird der Controller 2028 im Einklang mit der Cyberresilienzverordnung in den Verkehr gebracht. Im Jahr 2028 fällt bei beiden Controllern ein digitales Kommunikationsmodul aus. Der Hersteller liefert als Ersatzteil ein Ersatzmodul, das mit dem Original identisch ist und nach denselben Spezifikationen hergestellt wurde.

In beiden Fällen fällt das Ersatzmodul in den Anwendungsbereich der Ausnahme nach Artikel 2 Absatz 6. Das Ersatzteil selbst unterliegt nicht der Cyberresilienzverordnung, auch wenn es sich um ein Produkt mit digitalen Elementen handelt, da es eine identische Komponente in einem Produkt mit digitalen Elementen ersetzt. Die Reparatur stellt keine wesentliche Änderung des Produkts mit digitalen Elementen dar.

Beispiel 37: Ein Hersteller bringt im Jahr 2026, vor dem Inkrafttreten der Cyberresilienzverordnung, einen für industrielle Zwecke vorgesehenen Controller in den Verkehr. Im Jahr 2028 fällt in diesem Controller ein Kommunikationschip aus. Da dieser Chip nicht mehr hergestellt wird, liefert der Hersteller als Ersatzteil einen neueren Chip mit gleichwertigen Funktionen, aber mit einer anderen kryptografischen Implementierung und einem aktualisierten sicheren Boot-Mechanismus, damit die Kompatibilität gewahrt und der kontinuierliche Betrieb aufrechterhalten bleibt.

In diesem Fall kann der Ersatzchip nicht als identisch angesehen werden, da sich die Unterschiede bei der kryptografischen Implementierung und dem sicheren Boot-Mechanismus auf die Cybersicherheitsmerkmale des Chips auswirken. Er fällt daher nicht unter die Ausnahme nach Artikel 2 Absatz 6 und stellt ein Produkt mit digitalen Elementen dar, das der Cyberresilienzverordnung unterliegt. Die Konformität des Ersatzteils muss im Hinblick auf seine Zweckbestimmung bewertet werden, einschließlich seiner Rolle bei der Gewährleistung der Interoperabilität mit dem Produkt mit digitalen Elementen, das vor dem Inkrafttreten der Cyberresilienzverordnung in den Verkehr gebracht wurde.

Beispiel 38: Ein Hersteller bringt 2028 einen intelligenten Gebäude-Controller im Einklang mit der Cyberresilienzverordnung in den Verkehr. Im Jahr 2029 fällt das drahtlose Modul dieses Controllers aus. Da dieses Modul nicht mehr hergestellt wird, liefert der Hersteller als Ersatzteil ein neues Modul, das dieselbe Funktion unter Verwendung derselben Kommunikationsprotokolle und Sicherheitsmechanismen erfüllt, aber auf einem anderen Chipsatz beruht und über eine aktualisierte Firmware verfügt, die die für die Cybersicherheit möglicherweise relevanten Merkmale jedoch nicht verändert.

In diesem Fall kann das Ersatzmodul als identisch angesehen werden. Das Modul fällt daher unter die Ausnahme nach Artikel 2 Absatz 6 und unterliegt nicht der Cyberresilienzverordnung.

102. Die Ausnahme für Ersatzteile gilt unabhängig davon, ob das Ersatzteil eine Komponente in einem Produkt mit digitalen Elementen ersetzt oder ob es ein vollständiges Produkt mit digitalen Elementen ersetzt, das selbst Teil eines größeren Produkts ist, auch wenn dieses größere Produkt mit digitalen Elementen aus mehreren integrierten Komponenten besteht, sofern das Ersatzteil, wie in den vorstehenden Absätzen erläutert, explizit als Ersatzteil geliefert wird.

Beispiel 39: Im Jahr 2027 bringt ein Hersteller ein industrielles Automatisierungssystem in den Verkehr, zu dessen Bestandteilen eine speicherprogrammierbare Steuerung (SPS) gehört. Im Jahr 2031 fällt die Zentraleinheit (CPU) der SPS aus. Der Hersteller bietet zwei Reparaturoptionen an: i) Lieferung einer Ersatz-Zentraleinheit, die als identisch mit der ursprünglich installierten Zentraleinheit angesehen werden kann, oder ii) Lieferung einer kompletten Ersatz-SPS, die als identisch mit der ursprünglich installierten SPS angesehen werden kann. In jedem Fall wird die neue Komponente über den Kundendienstkanal des Herstellers als Ersatzteil geliefert, und das industrielle Automatisierungssystem, für welches die neue Komponente bestimmt ist, ist eindeutig angegeben. In beiden Fällen fällt der Austausch in den Anwendungsbereich der Ausnahme nach Artikel 2 Absatz 6, unabhängig davon, ob der Austausch eine Komponente innerhalb der SPS oder die gesamte SPS betrifft.

4.3. **Software-Aktualisierungen als wesentliche Änderungen**

103. Softwareentwicklung wohnt ein Wiederholungscharakter inne, wobei bereits in den Verkehr gebrachte Softwareprodukte mit digitalen Elementen häufig und kontinuierlich aktualisiert werden. In diesem Zusammenhang ist es sinnvoll, mehr Orientierungshilfen für die Feststellung zu geben, wann Software als wesentlich geändert zu betrachten ist. Diese Leitlinien sollen insbesondere Herstellern von Softwareprodukten mit digitalen Elementen, die Änderungen an ihren eigenen Produkten vornehmen, dabei helfen, festzustellen, ob es sich bei diesen Änderungen um eine wesentliche Änderung handelt.

104. In Erwägungsgrund 39 wird darauf hingewiesen, dass ein Produkt mit digitalen Elementen wesentlich geändert ist, wenn sich durch eine Änderung das Niveau des Cybersicherheitsrisikos ändert und wenn ein solches verändertes oder zusätzliches Risiko vom Hersteller bei seiner Risikobewertung und folglich bei der Umsetzung der grundlegenden Anforderungen nicht berücksichtigt wurde. Ein Hersteller sollte daher jeweils im Einzelfall prüfen, ob eine Software-Aktualisierung neue oder erhöhte Cybersicherheitsrisiken mit sich bringt und ob diese Risiken bereits in seiner Risikobewertung berücksichtigt wurden.

105. Integriert ein Hersteller in ein Produkt mit digitalen Elementen neue Funktionalitäten, die zu einer Änderung der Zweckbestimmung des Produkts insgesamt führen, ist es wahrscheinlich, dass der Hersteller solche Änderungen bei seiner Risikobewertung nicht berücksichtigt hat. Unter diesen Umständen würde die Änderung im Allgemeinen als wesentliche Änderung gelten.

Beispiel 40: Ein Hersteller bringt ein Dashboard in den Verkehr, das Daten von Maschinen erfasst und Trends und Warnmeldungen anzeigt, diese Maschinen jedoch nicht steuern kann. Anschließend entwickelt der Hersteller eine neue Version dieses Dashboards und führt Funktionen ein, auf deren Grundlage es auch Maschinen steuern kann, unter anderem durch die Anpassung der Betriebsparameter und das Wiedereinschalten der Maschinen nach Fehlerbedingungen. Infolge dieser Änderungen hat sich die Zweckbestimmung des Dashboards über das Maß hinaus weiterentwickelt, das in der Risikobewertung vorgesehen war. Das Dashboard hat sich also von einem Instrument zur Lageerfassung zu einem Produkt mit digitalen Elementen entwickelt, dessen bestimmungsgemäße Verwendung die operative Steuerung anderer Geräte umfasst. Das Dashboard wurde folglich wesentlich geändert.

Beispiel 41: Ein Hersteller bringt eine Verbrauchersoftware-Anwendung in den Verkehr, die dazu bestimmt ist, personenbezogene Daten wie E-Mails, Nachrichten oder Dokumente zu organisieren und anzuzeigen und grundlegende Such- und Filterfunktionen zu unterstützen. Anschließend bringt der Hersteller eine Aktualisierung heraus, auf deren Grundlage die Anwendung Nutzerinhalte automatisch analysieren kann, um Verhaltensprofile zu erstellen und automatisierte Entscheidungen zu treffen, die sich auf die Priorisierung, Unterdrückung oder Empfehlung von Inhalten ohne Eingreifen des Nutzers auswirken. Infolge dieser Änderung ändert sich die Zweckbestimmung der Software von einem nutzergesteuerten Informationsmanagement-Tool zu einem automatisierten Entscheidungssystem, was in der Risikobewertung nicht vorgesehen war. Die Anwendung wurde folglich wesentlich geändert.

106. Gleichzeitig ist es jedoch möglich, dass ein Hersteller schrittweise neue Funktionalitäten einführt, die bereits in seiner Risikobewertung enthalten sind oder die für sich genommen das Cybersicherheitsrisikoprofil des Produkts mit digitalen Elementen nicht verändern. Dies kann beispielsweise der Fall sein, wenn der Hersteller die Entwicklung dieser Funktionalitäten antizipiert, die damit verbundenen Risiken bereits beschrieben und bewertet und geeignete Risikominderungsmaßnahmen ergriffen hat, um die kontinuierliche Einhaltung der grundlegenden Anforderungen sicherzustellen. Dies kann auch der Fall sein, wenn mit den neuen Funktionalitäten keine Änderungen umgesetzt werden, die neue oder erhöhte Risiken mit sich bringen. Aktualisierungen dieser Art sollten daher nicht als wesentliche Änderungen angesehen werden, da sie das Cybersicherheitsrisiko nicht erhöhen und folglich die Umsetzung der grundlegenden Anforderungen nicht ändern.

Beispiel 42: Eine neue Messaging-Anwendung wird veröffentlicht, deren Funktionalität auf den Austausch von Nachrichten zwischen zwei Kommunikationspartnern beschränkt ist. Die Risikobewertung des Herstellers umfasst die spätere Einführung von Gruppennachrichten, einschließlich beispielsweise der erhöhten Komplexität des Nachrichten-Routings. Bei einer späteren Aktualisierung erweitert der Hersteller die Anwendung um eine Gruppen-Chat-Funktion, zusammen mit einer Administratorsteuerung und Moderations-Tools, die bereits in der ursprünglichen Konzeption vorgesehen und bewertet wurden. Mit der Aktualisierung werden Funktionen implementiert, die in den Anwendungsbereich der ursprünglichen Zweckbestimmung und Risikobewertung fallen. Die Messaging-Anwendung wurde folglich nicht wesentlich geändert.

Beispiel 43: Ein Produktionsüberwachungssystem wird mit aktivierten schreibgeschützten Dashboards in den Verkehr gebracht, wobei zwar automatisierte Steuerungsfunktionen in der Systemarchitektur vorhanden sind, aber deaktiviert bleiben. Die Risikobewertung des Herstellers erstreckt sich ausdrücklich auf die künftige Aktivierung automatisierter Regelkreise, einschließlich der Cybersicherheitsrisiken im Zusammenhang mit einer Regelung mit geschlossener Rückführung, sowie auf Schutzvorkehrungen wie Bediener-Override-Mechanismen und ausfallsichere Zustände. Bei einer späteren Aktualisierung aktiviert der Hersteller die automatischen Steuerungsfunktionen und die Schutzvorrichtungen, wie sie ursprünglich bewertet wurden. Das Produktionsüberwachungssystem wurde folglich nicht wesentlich geändert.

107. Umgekehrt können selbst begrenzte oder anscheinend geringfügige neue Funktionen erhebliche Cybersicherheitsrisiken mit sich bringen, die sich auf die Einhaltung der grundlegenden Anforderungen auswirken. Die Bewertung einer wesentlichen Änderung sollte sich daher nicht auf das Ausmaß oder die Komplexität der Änderung stützen, sondern auf ihre potenziellen negativen Auswirkungen auf das Cybersicherheitsrisikoprofil des Produkts mit digitalen Elementen und folglich auf die Umsetzung der grundlegenden Anforderungen.

Beispiel 44: Ein Hersteller führt eine Aktualisierung einer Softwareanwendung ein, indem er eine Funktion „Angemeldet bleiben" hinzufügt, bei der Authentifizierungs-Tokens lokal gespeichert werden, um die Benutzerfreundlichkeit zu verbessern. Obwohl die Funktionalität in ihrem Umfang begrenzt ist, bringt sie im Zusammenhang mit einem möglichen Diebstahl des Token, unbefugtem Zugriff und Session-Hijacking neue Risiken mit sich, die bei der Risikobewertung nicht berücksichtigt wurden. Die Aktualisierung wirkt sich daher auf die Einhaltung der grundlegenden Anforderungen aus. Die Software-Anwendung wurde wesentlich geändert.

Beispiel 45: Ein Hersteller fügt zu einem bestehenden Softwareprodukt mit digitalen Elementen eine neue Protokollierungs- und Diagnosefunktion hinzu, die den Export detaillierter Systemprotokolle zur Fehlerbehebung ermöglicht. Zwar erscheint die Funktionalität geringfügig, doch führt sie zur Erhebung und Speicherung sensibler Betriebsdaten in einem unverschlüsselten Format, wodurch Risiken der Datenexposition entstehen, die vorher nicht bewertet oder gemindert wurden. Die Änderung kann daher erhebliche Auswirkungen auf das Cybersicherheitsrisikoprofil des Produkts mit digitalen Elementen haben. Das Softwareprodukt mit digitalen Elementen wurde wesentlich geändert.

108. Im Einklang mit Erwägungsgrund 39 der Cyberresilienzverordnung sind Sicherheitsaktualisierungen im Allgemeinen nicht als wesentliche Änderungen anzusehen, da ihr Hauptzweck darin besteht, das mit dem Produkt mit digitalen Elementen verbundene Cybersicherheitsrisiko zu verringern. Eine Sicherheitsaktualisierung, die die Zweckbestimmung des Produkts nicht ändert und keine neuen Cybersicherheitsrisiken mit sich bringt, sollte daher nicht als wesentliche Änderung gelten, selbst wenn mit dieser Aktualisierung erhebliche technische Änderungen eingeführt werden. Dies gilt auch für den Fall, dass bestimmte Funktionalitäten ausschließlich zu dem Zweck geändert oder eingeschränkt werden, festgestellte Schwachstellen zu mindern und die kontinuierliche Einhaltung der grundlegenden Anforderungen sicherzustellen.

Beispiel 46: Ein Hersteller veröffentlicht eine Sicherheitsaktualisierung, um eine Schwachstelle in der Codebasis eines Produkts mit digitalen Elementen in der Form zu beheben, dass ein Eingabevalidierungsfehler berichtigt wird, der zu einem Pufferüberlauf führen könnte, oder ein Logik-Fehler behoben wird, der es ermöglicht, die Authentifizierung durch eine nicht ordnungsgemäße Validierung des Sitzungstokens zu umgehen. Durch die Aktualisierung wird die interne Implementierung der Software geändert, ohne dass sich dies auf die Zweckbestimmung dieses Produkts auswirkt oder eine neue Schwachstelle eingeführt wird. Eine solche Aktualisierung dient ausschließlich dazu, das Cybersicherheitsrisiko zu verringern. Die Sicherheitsaktualisierung sollte nicht als wesentliche Änderung betrachtet werden.

Beispiel 47: Ein Hersteller veröffentlicht eine Sicherheitsaktualisierung, die bestehende Sicherheitskonfigurationen stärkt, wie beispielsweise die Verschärfung der Firewall-Regeln, die Deaktivierung ungenutzter Netzwerk-Ports, die Änderung der Standard-Administrator-Passwortrichtlinien oder die Einführung einer obligatorischen Mehrfaktor-Authentifizierung, wenn eine solche Funktionalität bereits verfügbar oder vorgesehen war. Auch wenn die Aktualisierung Auswirkungen darauf haben kann, wie Nutzer das Produkt mit digitalen Elementen konfigurieren oder darauf zugreifen, ändert sich dadurch nichts an seiner Zweckbestimmung und es dient ausschließlich der Verbesserung seiner Sicherheit. Die Sicherheitsaktualisierung sollte nicht als wesentliche Änderung betrachtet werden.

Beispiel 48: Ein Hersteller bringt ein Softwareprodukt mit digitalen Elementen in den Verkehr, das die Kommunikation mithilfe eines konfigurierbaren Verschlüsselungsrahmens gewährleistet, der mehrere kryptografische Algorithmen und Schlüsselgrößen unterstützt, wie es in der technischen Dokumentation und der Risikobewertung des Produkts beschrieben ist. Die Risikobewertung deckt alle kryptografischen Optionen ab, die im Produkt mit digitalen Elementen bereitgestellt sind, und antizipiert, dass bestimmte Algorithmen künftig ausgemustert werden. Die Risikobewertung umfasst auch Risikominderungsmaßnahmen wie kryptografische Agilität, internes Schlüsselmanagement und Kompatibilitätstests. Angesichts neuer, die Kryptografie betreffende Leitlinien gibt der Hersteller eine Sicherheitsaktualisierung heraus, durch die ein veralteter Algorithmus deaktiviert und eine stärkere, bereits unterstützte Alternative aktiviert wird, ohne dass neue externe Abhängigkeiten eingeführt werden oder sich die Datenströme verändern. Da mit der Aktualisierung eine Sicherheitsmaßnahme umgesetzt wird, die als Teil der ursprünglichen Konzeption vorgesehen und bewertet wurde, und keine neuen Cybersicherheitsrisiken eingeführt werden, ist die Sicherheitsaktualisierung nicht als wesentliche Änderung zu betrachten.

109. Dagegen kann eine Sicherheitsaktualisierung als wesentliche Änderung gelten, wenn die Aktualisierung ungeachtet ihres Sicherheitsziels dazu führt, dass die Zweckbestimmung des Produkts mit digitalen Elementen über das ursprünglich vorgesehene Maß hinaus verändert wird oder neue oder erhöhte Cybersicherheitsrisiken mit sich bringt. Dies kann beispielsweise der Fall sein, wenn eine Aktualisierung die Grenzen oder die Abhängigkeitsstruktur des Produkts in einer Weise wesentlich verändert, die in der Risikobewertung nicht vorgesehen ist, beispielsweise durch eine wesentliche Änderung der Datenströme oder durch neue extern erreichbare Schnittstellen.

Beispiel 49: Ein Hersteller bringt ein Softwareprodukt mit digitalen Elementen in den Verkehr, das dazu bestimmt ist, eine lokale Dateiverschlüsselung für Daten bereitzustellen, die auf dem Gerät eines Nutzers gespeichert sind, und das es Nutzern ermöglicht, Dateien auf Anforderung zu verschlüsseln und zu entschlüsseln. Nach der Aufdeckung einer Sicherheitslücke im Verschlüsselungs-Workflow führt der Hersteller eine Sicherheitsaktualisierung durch, mit der die lokale Verschlüsselungsfunktionalität entfernt und stattdessen die Vorgabe eingeführt wird, dass alle Dateien auf einen vom Hersteller betriebenen Fernverschlüsselungsdienst hochgeladen, dort gespeichert und von diesem Dienst verarbeitet werden. Infolge dieser Änderung führt das Produkt mit digitalen Elementen nicht mehr die vorher vorhandene lokale Verschlüsselung durch, sondern dient stattdessen als Fernverschlüsselungs- und Datenverarbeitungsdienst. Obwohl die Aktualisierung aus Sicherheitsgründen vorgenommen wird, ändert sie die Zweckbestimmung dieses Produkts grundlegend in einer Weise, die in der Risikobewertung nicht vorgesehen ist, und gilt daher als wesentliche Änderung.

Beispiel 50: Ein Hersteller bringt ein Softwareprodukt mit digitalen Elementen in den Verkehr, das auf einem etablierten Verschlüsselungsprotokoll und einem intern verwalteten Schlüssellebenszyklus beruht, um die Kommunikation zwischen Komponenten des Produkts mit digitalen Elementen abzusichern. Angesichts neu festgestellter kryptografischer Schwachstellen gibt der Hersteller eine Sicherheitsaktualisierung heraus, die den bestehenden Verschlüsselungsmechanismus durch ein anderes Protokoll ersetzt, das die Nutzung eines von einem Dritten betriebenen externen Schlüsselverwaltungsdienstes erfordert. Infolge dieser Änderung werden die Abhängigkeiten und Datenströme des Produkts mit digitalen Elementen wesentlich verändert, wodurch neue externe Schnittstellen eingeführt werden und eine Abhängigkeit von Dienstleistungen Dritter entsteht, die bei der Risikobewertung nicht berücksichtigt wurde. Obwohl die Aktualisierung aus Sicherheitsgründen erfolgt, bringt sie neue Cybersicherheitsrisiken mit sich und gilt daher als wesentliche Änderung.

110. Wie unter Randnummer 104 dargelegt, sollte jeweils im Einzelfall geprüft werden, ob eine Software-Aktualisierung eine wesentliche Änderung darstellt. Bei der Durchführung dieser Bewertung können die Hersteller beispielsweise berücksichtigen, ob mit der Software-Aktualisierung:

a) neue Bedrohungsvektoren wie zusätzliche Schnittstellen, Kommunikationskanäle, Ausführungsumgebungen oder externe Abhängigkeiten implementiert werden, durch die es zu Bedrohungen kommen könnte,

b) neue Angriffsszenarien ermöglicht werden, einschließlich beispielsweise neuer Wege, über die ein unbefugter Zugriff, eine Manipulation, ein Eingriff oder ein Missbrauch des Produkts mit digitalen Elementen oder von ihm verarbeiteter Daten plausiblerweise erfolgen könnte,

c) sich die Wahrscheinlichkeit zuvor ermittelter Angriffsszenarien verändert, indem sich beispielsweise der Aufwand oder das Fachwissen, die erforderlich sind, um sie durchzuführen, verringert, die Exposition gegenüber nicht vertrauenswürdigen Akteuren zunimmt oder bestehende Schutzvorkehrungen geschwächt werden,

d) sich die potenziellen Auswirkungen zuvor ermittelter Angriffsszenarien verändern, beispielsweise das Ausmaß der betroffenen Daten oder Funktionen, die Schwere der betrieblichen, sicherheitsbezogenen oder wirtschaftlichen Folgen oder die Fähigkeit, einen Sicherheitsvorfall zu erkennen, einzudämmen oder seine Folgen zu bewältigen.

111. In einigen Fällen führt eine Software-Aktualisierung keine neuen Bedrohungsvektoren ein, ermöglicht keine neuen Angriffsszenarien und verändert die Wahrscheinlichkeit oder die Auswirkungen zuvor ermittelter Angriffsszenarien nicht wesentlich. Dies kann bedeuten, dass die Aktualisierung keine neuen oder erhöhten Cybersicherheitsrisiken mit sich bringt, sofern die Annahmen und Risikominderungsmaßnahmen, auf die sich die Risikobewertung stützt, weiterhin gültig und wirksam sind. Daher ist es wahrscheinlich, dass die Aktualisierung nicht als wesentliche Änderung einzustufen ist.

112. Umgekehrt können durch eine Software-Aktualisierung neue Bedrohungsvektoren eingeführt oder neue Angriffsszenarien ermöglicht werden oder sich die Wahrscheinlichkeit oder die Auswirkungen bestehender Angriffsszenarien wesentlich verändern. In solchen Fällen sollte der Hersteller die Cybersicherheitsrisiken des Produkts mit digitalen Elementen neu bewerten und feststellen, ob die grundlegenden Anforderungen weiterhin erfüllt sind, einschließlich der Frage, ob die Aktualisierung neue oder erhöhte Risiken mit sich bringt, die in der Risikobewertung nicht in Betracht gezogen sind.

113. Ob eine Software-Aktualisierung als wesentliche Änderung einzustufen ist, ist für die Feststellung relevant, ob bestimmte Pflichten im Rahmen der Cyberresilienzverordnung gelten, siehe hierzu Randnummer 91. Unabhängig von dieser Einstufung sind die Hersteller jedoch während des Unterstützungszeitraums weiterhin dafür verantwortlich, die Sicherheit von Software-Aktualisierungen und ihres Produkts mit digitalen Elementen im Einklang mit den Anforderungen an die Behandlung von Schwachstellen gemäß Anhang I Teil II der Cyberresilienzverordnung zu gewährleisten. Darüber hinaus sind die Hersteller gemäß Artikel 13 Absatz 7 und Artikel 31 Absatz 2 verpflichtet, die Risikobewertung und die technische Dokumentation genau, vollständig und kontinuierlich auf dem neuesten Stand zu halten, unabhängig davon, ob Software-Aktualisierungen als wesentliche Änderungen einzustufen sind oder nicht.

4.4. **Folgen einer wesentlichen Änderung**

114. Die Folgen einer wesentlichen Änderung, die von einem anderen Akteur als dem ursprünglichen Hersteller eines bereits in den Verkehr gebrachten Produkts mit digitalen Elementen vorgenommen wurde, sind Gegenstand der Artikel 21 und 22 der Cyberresilienzverordnung. Artikel 21 betrifft Einführer und Händler, während Artikel 22 jede natürliche oder juristische Person mit Ausnahme des Herstellers, Einführers oder Händlers betrifft.

115. Wird die wesentliche Änderung vom ursprünglichen Hersteller des Produkts mit digitalen Elementen vorgenommen, ergeben sich die Folgen aus dem allgemein etablierten Konzept der wesentlichen Änderung, auf das in Erwägungsgrund 41 der Cyberresilienzverordnung Bezug genommen und auf das in Abschnitt 2.1 des „Blue Guide“ näher eingegangen wird. In diesem Abschnitt heißt es, dass ein Produkt, an dem nach seinem Inverkehrbringen wesentliche Änderungen oder Überarbeitungen vorgenommen wurden, als neues Produkt anzusehen ist, wenn seine ursprüngliche Leistung, Verwendung oder Bauart geändert wurde, sich die Art der Gefahr verändert oder das Risikoniveau erhöht hat und das Produkt mit digitalen Elementen auf dem Markt bereitgestellt wird.

116. Die allgemein anerkannte Folge ist daher, dass eine Änderung eines Produkts mit digitalen Elementen, wenn sie als wesentliche Änderung einzustufen ist und das geänderte Produkt mit digitalen Elementen auf dem Markt bereitgestellt wird, für die Zwecke der Cyberresilienzverordnung als neues Produkt mit digitalen Elementen zu behandeln ist. Folglich stellt das Bereitstellen des wesentlich geänderten Produkts auf dem Markt ein neues Inverkehrbringen dar. Dies gilt unabhängig davon, ob die wesentliche Änderung vom ursprünglichen Hersteller oder von einer anderen Person vorgenommen wird. Um sicherzustellen, dass die Cyberresilienzverordnung in den verschiedenen Kategorien von Akteuren, die eine wesentliche Änderung vornehmen können, einheitlich und verhältnismäßig angewandt wird, wird in den folgenden Unterabschnitten auf die Verpflichtungen eingegangen, die sich für die Person ergeben, die die wesentliche Änderung vornimmt, wenn das wesentlich geänderte Produkt mit digitalen Elementen in den Verkehr gebracht wird. Die Folgen für den Unterstützungszeitraum des Produkts mit digitalen Elementen sind Gegenstand von Abschnitt 5 *Unterstützungszeitraum*.

4.4.1. *Wesentliche Änderungen, die von einer anderen Person als dem ursprünglichen Hersteller vorgenommen wurden*

117. Wird eine wesentliche Änderung an einem bereits in den Verkehr gebrachten Produkt mit digitalen Elementen von einer anderen natürlichen oder juristischen Person als dem Hersteller des Produkts mit digitalen Elementen vorgenommen, so gilt gemäß den Artikeln 21 und 22 die Person, die die wesentliche Änderung vornimmt und das geänderte Produkt mit digitalen Elementen auf dem Markt bereitstellt, als der Hersteller des geänderten Produkts mit digitalen Elementen, unabhängig davon, ob diese Person an der ursprünglichen Konzeption oder dem ursprünglichen Inverkehrbringen dieses Produkts beteiligt war.

118. In Artikel 22 wird ferner klargestellt, dass die Person, die die Änderung vornimmt, den in den Artikeln 13 und 14 festgelegten Pflichten nur in Bezug auf den Teil des Produkts mit digitalen Elementen unterliegt, der von der wesentlichen Änderung betroffen ist, sofern sich diese Änderung nicht auf die Cybersicherheit des Produkts mit digitalen Elementen in seiner Gesamtheit auswirkt.

119. Wenn sich eine wesentliche Änderung auf die Einhaltung der grundlegenden Anforderungen auswirkt, aber keine negativen Auswirkungen auf die Cybersicherheit des Produkts mit digitalen Elementen als Ganzes hat, unterliegt die Person, die die Änderung vornimmt, den Artikeln 13 (einschließlich der Verpflichtung, die Einhaltung der grundlegenden Anforderungen sicherzustellen und ein Konformitätsbewertungsverfahren durchzuführen) und 14 (Meldepflichten) nur in Bezug auf den Teil des Produkts mit digitalen Elementen, der wesentlich geändert wurde ([16]). Darüber hinaus gelten die Pflichten des ursprünglichen Herstellers im Rahmen der Cyberresilienzverordnung weiterhin für das in den Verkehr gebrachte Originalprodukt mit digitalen Elementen, wodurch sichergestellt ist, dass Schwachstellen kontinuierlich behandelt werden und die nicht geänderten Teile konform bleiben.

120. Ein Fall einer wesentlichen Änderung sollte nicht mit Fällen der Integration verwechselt werden, in denen eine Person Komponenten (gegebenenfalls auch durch Modifizierung) zu einem neuen Produkt mit digitalen Elementen zusammenbaut, das sie selbst in den Verkehr bringt. In solchen Fällen verändert der Integrator kein Produkt mit digitalen Elementen, das bereits von einem anderen Hersteller in den Verkehr gebracht wurde; vielmehr bringt er ein neues Produkt mit eigenen digitalen Elementen auf den Markt. Für die Zwecke der Cyberresilienzverordnung ist der Integrator der Hersteller dieses neuen Produkts mit digitalen Elementen und muss in Bezug auf das Produkt mit digitalen Elementen die Verordnung in ihrer Gesamtheit einhalten. Wenn der Hersteller Komponenten integriert, die der Cyberresilienzverordnung unterliegen, kann er sich auf die Aktivitäten stützen, die der Hersteller der Komponenten unternommen hat, um die Konformität zu gewährleisten, was ihm selbst die Einhaltung der Cyberresilienzverordnung erleichtert.

Beispiel 51: Ein Unternehmen kauft handelsübliche Mikrocontroller-Module und Konnektivitätskomponenten von Drittanbietern, entwickelt firmeneigene Firmware und ein Sensorpaket und kombiniert diese Komponenten zu einem vernetzten landwirtschaftlichen Überwachungsprodukt mit digitalen Elementen, das es in seinem eigenen Namen in den Verkehr bringt. Zwar hat das Unternehmen die zugrunde liegenden Mikrocontroller-Module verändert und mit anderen Komponenten kombiniert, doch hat es auf diese Weise nicht ein bereits in den Verkehr gebrachtes Produkt mit digitalen Elementen wesentlich geändert, sondern bringt vielmehr ein neues Produkt mit digitalen Elementen in den Verkehr. Das Unternehmen ist für die Zwecke der Cyberresilienzverordnung Hersteller der landwirtschaftlichen Überwachungseinrichtung und ist verpflichtet, die Verordnung in Bezug auf die landwirtschaftliche Überwachungseinrichtung als Ganzes einzuhalten.

([16]) Gemäß Abschnitt 2.1 des „Blue Guide“ ist es „nicht notwendig, Tests zu wiederholen und neue Unterlagen zu erstellen, die nicht von der Änderung betroffen sind. Die natürliche oder juristische Person, die Veränderungen an dem Produkt vornimmt oder vornehmen lässt, muss nachweisen, dass nicht alle Aspekte der technischen Unterlagen aktualisiert werden müssen. Die natürliche oder juristische Person, die Änderungen an dem Produkt vornimmt oder vornehmen lässt, ist für die Konformität des geänderten Produkts verantwortlich und stellt eine Konformitätserklärung aus, selbst wenn sie bereits vorhandene Prüfungen und technische Unterlagen verwendet.“

121. Wenn sich eine wesentliche Änderung, die von einer anderen Person als dem ursprünglichen Hersteller vorgenommen wurde, negativ auf die Cybersicherheit des Produkts mit digitalen Elementen als Ganzes auswirkt, beispielsweise weil die Änderung nicht mehr auf eine bestimmte Komponente oder ein bestimmtes Teilsystem ausgerichtet oder darauf beschränkt ist, sollte das geänderte Produkt mit digitalen Elementen, das auf dem Markt bereitgestellt wird, als neues Produkt mit digitalen Elementen behandelt werden, das in seiner Gesamtheit der Cyberresilienzverordnung unterliegt. In solchen Fällen hat sich das allgemeine Cybersicherheitsrisikoprofil dieses Produkts verändert, und die Änderung kann nicht bewertet werden, ohne das Produkt mit digitalen Elementen als Ganzes zu berücksichtigen. Die Person, die die Änderung vornimmt, unterliegt in Bezug auf das geänderte Produkt mit digitalen Elementen als Ganzes den Pflichten eines Herstellers gemäß den Artikeln 13 und 14.

4.4.2. *Wesentliche Änderungen, die vom ursprünglichen Hersteller vorgenommen wurden*

122. Wird die wesentliche Änderung vom ursprünglichen Hersteller vorgenommen, auch im Zusammenhang mit der iterativen Entwicklung von Softwareprodukten mit digitalen Elementen, bleibt dieser Hersteller für die Zwecke der Cyberresilienzverordnung der Hersteller. Das wesentlich geänderte Produkt mit digitalen Elementen gilt jedoch als neu in den Verkehr gebracht.

123. Gemäß Abschnitt 2.1 des „Blue Guide“ kann der ursprüngliche Hersteller, der das wesentlich geänderte Produkt mit digitalen Elementen in den Verkehr bringt, bereits vorhandene Unterlagen und Testergebnisse zu Aspekten des Produkts mit digitalen Elementen, die nicht von der wesentlichen Änderung betroffen sind, weiterverwenden. Insbesondere wenn der Hersteller wesentlich geänderte Versionen desselben Produkts mit digitalen Elementen in den Verkehr bringt, sollte sich das Konformitätsbewertungsverfahren auf die wesentlich geänderten Teile des Produkts mit digitalen Elementen konzentrieren. Ebenso sollte sich die Konformitätsbewertungsstelle, wenn eine Konformitätsbewertung durch Dritte durchgeführt wird, bei ihrer Bewertung auf die wesentlich geänderten Teile konzentrieren. Für nicht geänderte Teile des Produkts mit digitalen Elementen können vorhandene Unterlagen und Testergebnisse weiterverwendet werden.

124. Die im vorstehenden Unterabschnitt dargelegten Verhältnismäßigkeitserwägungen gelten auch für wesentliche Änderungen, die vom ursprünglichen Hersteller eines vor dem 11. Dezember 2027 in den Verkehr gebrachten Produkts mit digitalen Elementen vorgenommen wurden. Eine solche vom ursprünglichen Hersteller vorgenommene wesentliche Änderung erfordert für sich genommen nicht, dass der Hersteller das gesamte Produkt mit digitalen Elementen, das vor diesem Datum in den Verkehr gebracht wurde, vollständig mit der Cyberresilienzverordnung in Einklang bringt, es sei denn, die Änderung wirkt sich negativ auf die Cybersicherheit des Produkts mit digitalen Elementen als Ganzes aus. Hat die Änderung keine Auswirkungen auf die Cybersicherheit des Produkts mit digitalen Elementen als Ganzes, so sollten die Pflichten des ursprünglichen Herstellers in Bezug auf die Änderung auf die wesentlich geänderten Teile beschränkt werden.

5. **UNTERSTÜTZUNGSZEITRAUM**

125. In Artikel 13 Absatz 8 der Cyberresilienzverordnung ist vorgeschrieben, dass die Hersteller den Unterstützungszeitraum festlegen, in dem Schwachstellen des Produkts mit digitalen Elementen, einschließlich seiner Komponenten, wirksam und im Einklang mit den grundlegenden Anforderungen in Anhang I Teil II behandelt werden. Der Unterstützungszeitraum spiegelt die Dauer der voraussichtlichen Nutzung des Produkts mit digitalen Elementen wider und sollte entsprechend den Kriterien in Artikel 13 Absatz 8 festgelegt werden, insbesondere entsprechend den angemessenen Erwartungen der Nutzer, der Art des Produkts mit digitalen Elementen, einschließlich seiner Zweckbestimmung, sowie den einschlägigen Rechtsvorschriften der Union zur Festlegung der Lebensdauer von Produkten mit digitalen Elementen ([17]). Insgesamt sind diese Kriterien in einer Weise zu berücksichtigen, die die Verhältnismäßigkeit bei der Festlegung des Unterstützungszeitraums gewährleistet.

([17]) Weitere Kriterien, die entsprechend Artikel 13 Absatz 8 berücksichtigt werden können, sind unter anderem die Unterstützungszeiträume für Produkte mit digitalen Elementen mit einer ähnlichen Funktionalität, die von anderen Herstellern in den Verkehr gebracht werden, die Verfügbarkeit der Betriebsumgebung, die Unterstützungszeiträume für integrierte Komponenten, die Kernfunktionen bereitstellen und von Dritten bezogen werden, sowie die einschlägigen Leitlinien der Gruppe zur administrativen Zusammenarbeit (ADCO) im Rahmen der Cyberresilienzverordnung und der Kommission.

126. Gemäß Artikel 13 Absatz 8 muss der Unterstützungszeitraum mindestens fünf Jahre betragen, es sei denn, es wird davon ausgegangen, dass das Produkt mit digitalen Elementen weniger als fünf Jahre im Betrieb ist; dann muss der Unterstützungszeitraum der voraussichtlichen Nutzungsdauer entsprechen. Der Mindestunterstützungszeitraum dient folglich nur als Schutzmaßnahme, mit der sichergestellt wird, dass Schwachstellen über einen ausreichend langen Zeitraum behandelt werden, während gleichzeitig den Herstellern ermöglicht wird, Produkte mit digitalen Elementen mit einer tatsächlich kürzeren voraussichtlichen Nutzungsdauer zu berücksichtigen. Erwägungsgrund 60 bietet diesbezüglich weitere Orientierung, indem dort ausgeführt wird, dass bei Produkten mit digitalen Elementen, bei denen nach vernünftigem Ermessen davon auszugehen ist, dass sie länger als fünf Jahre verwendet werden, die Unterstützungszeiträume entsprechend länger sein sollten. Ein Unterstützungszeitraum von fünf Jahren ist daher nicht als Standard für alle Produkte mit digitalen Elementen zu betrachten. Stattdessen sollte der Hersteller den angemessenen Unterstützungszeitraum unter Berücksichtigung der in Artikel 13 Absatz 8 genannten Kriterien festlegen.

127. Gemäß Artikel 13 Absatz 19 müssen die Hersteller zum Zeitpunkt des Kaufs in klarer und verständlicher Weise das Enddatum des Unterstützungszeitraums (mindestens Monat und Jahr) angeben. Außerdem müssen die Hersteller den Nutzern am Ende des Unterstützungszeitraums eine entsprechende Mitteilung anzeigen, sofern dies angesichts der Art des Produkts mit digitalen Elementen technisch machbar ist. Diese Verpflichtung soll den Nutzern Transparenz in Bezug auf die Dauer bieten, für die sie eine Sicherheitsunterstützung erwarten können.

128. Bei Softwareprodukten mit digitalen Elementen, die häufig iterativ entwickelt und herausgegeben werden und von denen häufig im Laufe der Zeit wesentlich geänderte Versionen in den Verkehr gebracht werden können, ist der Unterstützungszeitraum im Lichte dieses Entwicklungsmodells zu verstehen. Für jede wesentlich geänderte Version eines in den Verkehr gebrachten Softwareprodukts mit digitalen Elementen muss ein angegebener Unterstützungszeitraum gelten, der Artikel 13 Absatz 8 entspricht. Dies schließt den Mindestunterstützungszeitraum von fünf Jahren ein, es sei denn, die voraussichtliche Nutzungsdauer dieser Version ist nachweislich kürzer, wie auch in Erwägungsgrund 60 klargestellt wird. Im Abschnitt *5.1 Wesentliche Änderungen und Unterstützungszeitraum* wird ferner klargestellt, dass in Fällen, in denen die wesentliche Änderung nicht zu Änderungen der Faktoren führt, die ursprünglich die voraussichtliche Nutzungsdauer des Produkts mit digitalen Elementen bestimmt haben, der ursprüngliche Unterstützungszeitraum unberührt bleibt (d. h. auch in Fällen, in denen der verbleibende Unterstützungszeitraum weniger als fünf Jahre beträgt).

129. Artikel 13 Absatz 10 bietet Flexibilität für Softwareprodukte mit digitalen Elementen, indem Herstellern gestattet wird, unter bestimmten Bedingungen die Einhaltung der Anforderungen an die Behandlung von Schwachstellen gemäß Anhang I Teil II Nummer 2 (Behandeln und Beheben von Schwachstellen) nur für die Version des Softwareprodukts mit digitalen Elementen sicherzustellen, die zuletzt in den Verkehr gebracht wurde. Dies ist zulässig, wenn die Nutzer zuvor in den Verkehr gebrachter Versionen kostenlos Zugang zu der zuletzt in den Verkehr gebrachten Version haben und ihnen keine zusätzlichen Kosten für die Anpassung der Hardware- und Softwareumgebung entstehen, in der sie die Originalversion dieses Produkts verwenden.

130. Für die Zwecke des Artikels 13 Absatz 10 sollte der Begriff „zusätzliche Kosten“ auf praktische und verhältnismäßige Weise ausgelegt werden, wobei normale und erwartete Verfahren bei Wartung und Betrieb der Software zu berücksichtigen sind. Sie umfassen nicht den angemessenen operativen Aufwand, der mit der Anwendung von Software-Aktualisierungen oder der Aufrechterhaltung einer sicheren Betriebsumgebung verbunden ist, beispielsweise Arbeitszeit, Routineprüfungen, Konfigurationsanpassungen oder Upgrades zugrunde liegender Softwareabhängigkeiten, die erforderlich sind, um mit Komponenten am Ende ihrer Lebensdauer umzugehen oder bekannte Sicherheitslücken zu beheben. Stattdessen bezieht sich der Begriff „zusätzliche Kosten“ auf Belastungen, die über das hinausgehen, was normalerweise im Zusammenhang mit Software-Aktualisierungen zu erwarten ist, wie beispielsweise der obligatorische Erwerb neuer Hardware, der Austausch von Infrastruktur oder grundlegende Änderungen der Betriebsumgebung.

131. Bei sich ständig weiterentwickelnden Softwareprodukten mit digitalen Elementen kann es sein, dass die Hersteller in relativ kurzen Zeitabständen sukzessive wesentlich geänderte Versionen in den Verkehr bringen und erwarten, dass die Nutzer diese regelmäßig aktualisieren. In solchen Fällen muss der angegebene Unterstützungszeitraum für jede wesentlich geänderte Version zum Zeitpunkt des Inverkehrbringens mit Artikel 13 Absatz 8 im Einklang stehen. Mit anderen Worten, der Hersteller muss für diese wesentlich geänderte Version einen neuen Unterstützungszeitraum angeben. Die Hersteller können sich jedoch auf Artikel 13 Absatz 10 berufen, um das Behandeln und Beheben von Schwachstellen für frühere Versionen einzustellen, sobald die Nutzer in der Lage sind, kostenlos und

ohne zusätzliche Kosten, wie vorstehend ausgeführt, auf eine neuere Version aufzurüsten, selbst wenn dies zu einem kürzeren effektiven Unterstützungszeitraum für diese früheren Versionen führt ([18]). Der Hersteller unterliegt weiterhin den anderen Anforderungen an die Behandlung von Schwachstellen gemäß Anhang I Teil II sowie den Meldepflichten gemäß Artikel 14. Wie auch in Erwägungsgrund 40 erläutert, umfassen diese Anforderungen unter anderem für alle nachfolgenden wesentlich geänderten Versionen des in den Verkehr gebrachten Softwareprodukts mit digitalen Elementen: i) über eine Strategie zur abgestimmten Offenlegung von Schwachstellen zu verfügen; und ii) Vorkehrungen getroffen haben, um den Informationsaustausch über potenzielle Schwachstellen zu erleichtern ([19]).

Beispiel 52: Ein Hersteller bringt in der EU ein Smartphone-Modell in den Verkehr und gibt einen Unterstützungszeitraum von X Jahren ab dem Datum des Inverkehrbringens an, in dem er Sicherheitsaktualisierungen zur Behebung von Schwachstellen bereitstellt. In diesem Zeitraum veröffentlicht der Hersteller regelmäßige Software-Aktualisierungen und wesentlich geänderte Versionen des Betriebssystems, die die Nutzer kostenlos installieren können, ohne neue Hardware zu benötigen.

Der Hersteller kann gemäß Artikel 13 Absatz 10 Schwachstellen der neuesten Version des für dieses Smartphone-Modell bereitgestellten Betriebssystems behandeln und beheben, sofern frühere Versionen kostenlos und ohne zusätzliche Kosten nachgerüstet werden können. Für die Dauer des Unterstützungszeitraums unterliegt der Hersteller weiterhin den anderen Anforderungen an die Behandlung von Schwachstellen, darunter Maßnahmen zur koordinierten Offenlegung von Schwachstellen und zum Informationsaustausch.

Beispiel 53: Ein Hersteller bringt ein Unternehmenssoftwareprodukt mit digitalen Elementen in den Verkehr und veröffentlicht alle paar Monate wesentlich geänderte Versionen, die Sicherheitsverbesserungen, neue Funktionen und die Kompatibilität mit aktualisierten Betriebssystemen und Plattformen widerspiegeln. Jede Version wird mit einem angegebenen Unterstützungszeitraum gemäß Artikel 13 Absatz 8 in den Verkehr gebracht. Der Hersteller erwartet von den Nutzern eine regelmäßige Aufrüstung im Rahmen des Normalbetriebs und bietet kostenlosen Zugang zur jeweils neuesten Version. Die Anwendung von Aufrüstungen kann einen angemessenen operativen Aufwand erfordern, beispielsweise Tests oder Konfigurationsanpassungen, geht jedoch nicht mit zusätzlichen Kosten einher, etwa für den Erwerb neuer Hardware oder grundlegende Infrastrukturänderungen. In diesem Zusammenhang kann sich der Hersteller auf Artikel 13 Absatz 10 berufen, um die Behandlung und Behebung von Schwachstellen für frühere Versionen einzustellen, sobald die Nutzer auf die neueste Version aufrüsten können, und gleichzeitig die anderen Anforderungen an die Behandlung von Schwachstellen für alle nachfolgenden wesentlich geänderten Versionen weiterhin zu erfüllen.

5.1. **Wesentliche Änderungen und Unterstützungszeitraum**

132. Wenn, wie in Abschnitt 4.4 *Folgen einer wesentlichen Änderung* dargelegt, eine Änderung eines Produkts mit digitalen Elementen als wesentliche Änderung gilt und das geänderte Produkt mit digitalen Elementen auf dem Markt bereitgestellt wird, ist dieses für die Zwecke der Cyberresilienzverordnung als neues Produkt zu behandeln, und das Bereitstellen des wesentlich geänderten Produkts mit digitalen Elementen auf dem Markt stellt ein neues Inverkehrbringen dar. Folglich sollte klargestellt werden, wie sich dieses neue Inverkehrbringen auf den Unterstützungszeitraum des wesentlich geänderten Produkts mit digitalen Elementen auswirkt.

133. Der Unterstützungszeitraum für ein wesentlich geändertes Produkt mit digitalen Elementen sollte unter Bezugnahme auf die voraussichtliche Nutzungsdauer des Produkts unter Berücksichtigung der in Artikel 13 Absatz 8 der Cyberresilienzverordnung angegebenen Kriterien festgelegt werden. Eine wesentliche Änderung sollte daher eine Neubewertung anhand dieser Kriterien erfordern, führt jedoch nicht automatisch dazu, dass der Unterstützungszeitraum neu festgesetzt oder sogar verlängert wird. Die entscheidende Frage ist, ob sich die wesentliche Änderung auf die Faktoren auswirkt, über die sich ursprünglich die voraussichtliche Nutzungsdauer dieses Produkts und damit der ursprüngliche Unterstützungszeitraum bestimmt haben.

([18]) Es sei daran erinnert, dass die Hersteller gemäß Artikel 13 Absatz 19 verpflichtet sind, den Nutzern, sofern dies angesichts der Art des Produkts mit digitalen Elementen technisch machbar ist, eine Mitteilung anzuzeigen, um sie darüber zu unterrichten, dass das Ende des Unterstützungszeitraums ihres Produkts mit digitalen Elementen erreicht ist. Wenn die Behandlung und Behebung von Schwachstellen für frühere Versionen eingestellt wird, so wird folglich erwartet, dass Nutzer, die nicht auf die neueste Version aufgerüstet wurden, informiert werden, sofern dies technisch machbar ist.

([19]) Es sei darauf hingewiesen, dass es den Herstellern auch in Fällen, in denen die Nutzer ohne zusätzliche Kosten auf die neueste Version der Software aufrüsten können, freisteht, auch weiterhin Schwachstellen in früheren Versionen dieser Software zu behandeln und zu beheben, auch gegen Entgelt oder im Rahmen anderer kommerzieller Vereinbarungen. Die Hersteller werden durch die Cyberresilienzverordnung nicht dazu verpflichtet, Sicherheitsaktualisierungen für solche früheren Versionen kostenlos bereitzustellen.

134. Wenn sich die wesentliche Änderung nicht auf diese Faktoren auswirkt, deuten die in Artikel 13 Absatz 8 festgelegten Kriterien weiterhin auf dieselbe voraussichtliche Nutzungsdauer wie ursprünglich festgelegt hin, und der Unterstützungszeitraum des geänderten Produkts mit digitalen Elementen sollte der verbleibenden voraussichtlichen Nutzungsdauer des Produkts in der ursprünglich in den Verkehr gebrachten Form entsprechen. Dies ist in der Regel der Fall, wenn die voraussichtliche Nutzungsdauer in erster Linie durch Faktoren bestimmt wurde, die durch die Änderung nicht verändert werden, wie beispielsweise die physische Haltbarkeit von Hardwarekomponenten, wenn die wesentliche Änderung nur die Funktionalität der Software oder Back-End-Dienste betrifft.

Beispiel 54: Ein Hersteller bringt einen Staubsauger-Roboter mit einer voraussichtlichen Nutzungsdauer von X Jahren in den Verkehr, die auf der Grundlage der Art des Produkts mit digitalen Elementen, einschließlich der physischen Haltbarkeit und der Verschleißeigenschaften der Hardwarekomponenten, und unter Berücksichtigung angemessener Erwartungen der Nutzer in Bezug auf die Lebensdauer dieses Produkts bestimmt wird. Der Hersteller legt einen Unterstützungszeitraum von X Jahren fest. Nach Y Jahren veröffentlicht der Hersteller eine Software-Aktualisierung, die als wesentliche Änderung einzustufen ist und mit der neue Reinigungsmodi und Navigationsfunktionen hinzugefügt werden. Die Software-Aktualisierung wirkt sich nicht auf die physische Haltbarkeit der Hardware aus und ändert nichts an den angemessenen Erwartungen der Nutzer in Bezug auf die Lebensdauer dieses Produkts. Gemäß den Kriterien nach Artikel 13 Absatz 8 wird daher weiterhin von derselben voraussichtlichen Nutzungsdauer ausgegangen. Der Unterstützungszeitraum des geänderten Produkts mit digitalen Elementen entspricht dem verbleibenden Zeitraum der ursprünglich festgelegten voraussichtlichen Nutzungsdauer.

Beispiel 55: Ein Hersteller bringt ein komplexes Industriemaschinenprodukt mit digitalen Elementen mit einem Cloud-Back-End in den Verkehr, das eine Datenfernverarbeitungslösung darstellt. Die voraussichtliche Nutzungsdauer beträgt X Jahre und wird unter Berücksichtigung angemessener Nutzererwartungen und der Art des Produkts mit digitalen Elementen wie der physischen Haltbarkeit der Maschinenhardware und des erwarteten Verschleißes bestimmt. Der Unterstützungszeitraum wird an die voraussichtliche Nutzungsdauer von X Jahren angepasst. Nach Y Jahren gestaltet der Hersteller das Cloud-Back-End (die Datenfernverarbeitungslösung) neu und führt neue APIs und Datenströme in einer Weise ein, die als wesentliche Änderung des Produkts mit digitalen Elementen einzustufen ist, ohne dass dies die Art dieses Produkts ändert oder die Erwartungen der Nutzer beeinflusst. Gemäß den Kriterien nach Artikel 13 Absatz 8 wird daher weiterhin von derselben voraussichtlichen Nutzungsdauer ausgegangen. Der Unterstützungszeitraum des geänderten Produkts mit digitalen Elementen entspricht dem verbleibenden Zeitraum der ursprünglich festgelegten voraussichtlichen Nutzungsdauer.

135. Wenn sich die wesentliche Änderung auf die Faktoren auswirkt, die ursprünglich die voraussichtliche Nutzungsdauer des Produkts mit digitalen Elementen bestimmt haben, sollte der Hersteller den Unterstützungszeitraum neu berechnen, um der neuen voraussichtlichen Nutzungsdauer Rechnung zu tragen, und die Kriterien nach Artikel 13 Absatz 8 entsprechend anwenden. Dies kann beispielsweise der Fall sein, wenn erneuernde Hardwareänderungen die Lebensdauer dieses Produkts verlängern oder wenn die Kernsoftware dieses Produkts erheblich umprogrammiert oder umgeschrieben wird, wodurch sich seine voraussichtliche Nutzungsdauer wesentlich ändert ([20]).

Beispiel 56: Ein Hersteller bringt eine speicherprogrammierbare Steuerung (SPS) mit einer voraussichtlichen Nutzungsdauer von X Jahren in den Verkehr, die in erster Linie auf der Grundlage der Art des Produkts mit digitalen Elementen und der Haltbarkeit der zugrunde liegenden Hardware bestimmt wird. Der Unterstützungszeitraum wird entsprechend festgelegt. Mehrere Jahre nach dem erstmaligen Inverkehrbringen nimmt der Hersteller eine wesentliche Änderung vor, die darin besteht, die eingebettete IT-Plattform der SPS, einschließlich Prozessor, Speicher und Laufzeitumgebung, durch eine neue Generation von Komponenten zu ersetzen, die für eine deutlich längere Lebensdauer konzipiert sind. Infolge der Änderung ändern sich die angemessenen Erwartungen der Nutzer und die Art des Produkts mit digitalen Elementen: Der Nutzer der SPS kann nun vernünftigerweise erwarten, dass die SPS über ihre ursprünglich angegebene voraussichtliche Nutzungsdauer hinaus produktiv genutzt werden kann, was durch die neue Rechenplattform unterstützt wird. Gemäß den Kriterien nach Artikel 13 Absatz 8 ist folglich von einer längeren voraussichtlichen Nutzungsdauer auszugehen, und der Hersteller berechnet den Unterstützungszeitraum für diese spezifische SPS dementsprechend neu.

6. **WICHTIGE UND KRITISCHE PRODUKTE MIT DIGITALEN ELEMENTEN**

136. In Artikel 7 Absatz 1 der Cyberresilienzverordnung ist festgelegt, dass Produkte mit digitalen Elementen, die die Kernfunktionen einer in Anhang III der Verordnung aufgeführten Produktkategorie aufweisen, als „wichtige Produkte mit digitalen Elementen“ gelten. In Anhang III werden wichtige Produkte mit digitalen Elementen weiter in die Klassen I und II unterteilt. Ebenso ist in Artikel 8 Absatz 1 festgelegt, dass Produkte mit digitalen Elementen, die die Kernfunktionen einer in Anhang IV der Cyberresilienzverordnung aufgeführten Produktkategorie aufweisen, als „kritische Produkte mit digitalen Elementen“ gelten ([21]).

([20]) Es sei daran erinnert, dass, wie in Abschnitt 4.1 *Physische Reparaturen* dargelegt, Überholungs-, Wartungs- oder Reparaturarbeiten in der Regel nicht als wesentliche Änderungen gelten.

([21]) Die Durchführungsverordnung (EU) 2025/2392 der Kommission enthält die technische Beschreibung der Kategorien wichtiger und kritischer Produkte.

137. Die Einstufung eines Produkts mit digitalen Elementen als wichtig oder kritisch oder umgekehrt als zur Kategorie „Standard“ ([22]) gehörend ist für die Bestimmung des Konformitätsbewertungsverfahrens von Bedeutung, das der Hersteller gemäß Artikel 32 befolgen muss, bevor er dieses Produkt mit digitalen Elementen in den Verkehr bringen darf. Insbesondere kann für Produkte mit digitalen Elementen in der Standardkategorie stets das interne Kontrollverfahren auf der Grundlage von Modul A („Selbstbewertung“) genutzt werden ([23]). Wichtige Produkte mit digitalen Elementen der Klassen I oder II und kritische Produkte mit digitalen Elementen unterliegen strengeren Konformitätsbewertungsverfahren. Dies gilt nicht für in den Verkehr gebrachte wichtige Produkte mit digitalen Elementen der Klassen I oder II, die als freie und quelloffene Software gelten und für die die Hersteller gemäß Artikel 32 Absatz 5 entsprechend den Verfahren der Standardkategorie vorgehen dürfen.

138. Bei der Festlegung des anzuwendenden Konformitätsbewertungsverfahrens ist daher für den Hersteller der Begriff der Kernfunktion von entscheidender Bedeutung. Dieser Begriff ist in der Cyberresilienzverordnung jedoch nicht ausdrücklich definiert. Produkte mit digitalen Elementen können eine Reihe von Funktionen erfüllen, von denen einige die Kernfunktionen des Produkts ergänzen können und sich nicht auf die Einstufung des Produkts als Standardprodukt/wichtiges Produkt der Klasse I/wichtiges Produkt der Klasse II/kritisches Produkt auswirken sollten. Daher ist es sinnvoll, weitere Orientierungshilfe zu bieten, um die Hersteller bei der ordnungsgemäßen Durchführung der einschlägigen Konformitätsbewertungsverfahren zu unterstützen und es den Marktüberwachungsbehörden einfacher zu machen, die Cyberresilienzverordnung in der gesamten EU harmonisiert durchzusetzen.

6.1. **Kernfunktionen**

139. Als Kernfunktionen eines Produkts mit digitalen Elementen sind die Hauptmerkmale und technischen Fähigkeiten dieses Produkts zu verstehen, ohne die es nicht in der Lage wäre, seine Zweckbestimmung zu erfüllen. Sie können unter Berücksichtigung des spezifischen Kontexts und der Nutzungsbedingungen dieses Produkts bewertet werden, wobei unter anderem die Informationen zu berücksichtigen sind, die der Hersteller in der Gebrauchsanleitung, im Werbe- oder Verkaufsmaterial und in Erklärungen sowie in der technischen Dokumentation bereitstellt.

Beispiel 57: Ein Softwareprodukt mit digitalen Elementen bietet eine Abstraktionsschicht über der zugrunde liegenden Hardware und verwaltet die Ausführung von Softwarekomponenten. Zu seinen Hauptfunktionen gehören Hardware- und Peripherieinitialisierung, Prozess- und Speichermanagement, Eingabe-Ausgabe-Steuerung, Planung, Ressourcenzuweisung und die Exposition von Systemdiensten und Anwendungsprogramm-Schnittstellen (API), über die Anwendungen mit den Hardware- und Softwareressourcen des Geräts interagieren. Aus der technischen Dokumentation geht hervor, dass das Produkt mit digitalen Elementen Rechenressourcen orchestriert, Systemkonfigurationen durchsetzt und standardisierte Schnittstellen für Softwaremodule und angeschlossene Peripheriegeräte bereitstellt. Der Hersteller betont, dass sich die Plattform durch diese Funktionen als zentrale Softwareumgebung einsetzen lässt, in der Anwendungen zuverlässig betrieben werden können. Das Produkt mit digitalen Elementen verfügt über die Kernfunktionen eines Betriebssystems gemäß Anhang I Nummer 11 der Durchführungsverordnung (EU) 2025/2392.

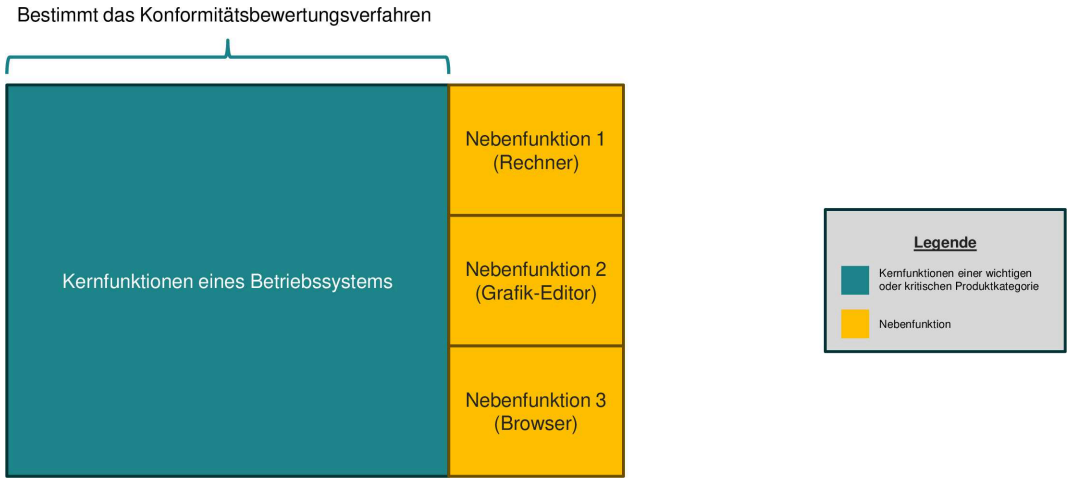
140. Die Funktionalität eines Produkts mit digitalen Elementen ist selten ausschließlich auf seine Kernfunktionen beschränkt, da Produkte mit digitalen Elementen häufig – wenn nicht gar immer – zusätzliche Funktionen erfüllen, die nicht zu den Kernfunktionen des Produkts beitragen. Dazu kann auch die Integration von Komponenten gehören, die selbst die Funktionalität eines anderen wichtigen oder kritischen Produkts mit digitalen Elementen aufweisen. Die Tatsache, dass ein Produkt mit digitalen Elementen andere oder zusätzliche Funktionen ausführt, die sich von denen, die in den technischen Beschreibungen wichtiger oder kritischer Produkte mit digitalen Elementen beschriebenen Funktionen aufgeführt sind, unterscheiden oder diese ergänzen, schließt jedoch für sich genommen nicht aus, dass das Produkt über solche Kernfunktionen verfügt.

([22]) Der Begriff „Standardkategorie“ ist kein in der Cyberresilienzverordnung definierter Begriff. Die Verwendung des Begriffs in diesem Dokument bezieht sich auf Produkte mit digitalen Elementen, die nicht die Kernfunktionen einer in den Anhängen III oder IV der Cyberresilienzverordnung aufgeführten Produktkategorie aufweisen und daher dem Konformitätsbewertungsverfahren nach Artikel 32 Absatz 1 unterliegen.

([23]) Der Hersteller kann sich jedoch stets für ein strengeres Konformitätsbewertungsverfahren als die in Artikel 32 Absatz 1 genannten entscheiden.

Abbildung 2

Schematische Darstellung„ wie sich über die Kernfunktionen, und nicht die Nebenfunktionen, das Konformitätsbewertungsverfahren bestimmt



141. Es ist möglich, dass ein Produkt mit digitalen Elementen die Funktionen einer wichtigen oder kritischen Produktkategorie ausführen kann, aber dennoch Kernfunktionen aufweist, die sich von denen einer solchen Produktkategorie unterscheiden. In solchen Fällen würde dieses Produkt mit digitalen Elementen nicht als wichtiges oder kritisches Produkt mit digitalen Elementen gelten. Wie in Artikel 7 Absatz 1 der Cyberresilienzverordnung für wichtige Produkte mit digitalen Elementen ausdrücklich festgelegt ist (wobei dieselbe Logik auch auf kritische Produkte mit digitalen Elementen anzuwenden ist), macht die bloße Integration eines wichtigen oder kritischen Produkts mit digitalen Elementen für sich genommen das Produkt mit digitalen Elementen nicht zu einem wichtigen oder kritischen Produkt mit digitalen Elementen.

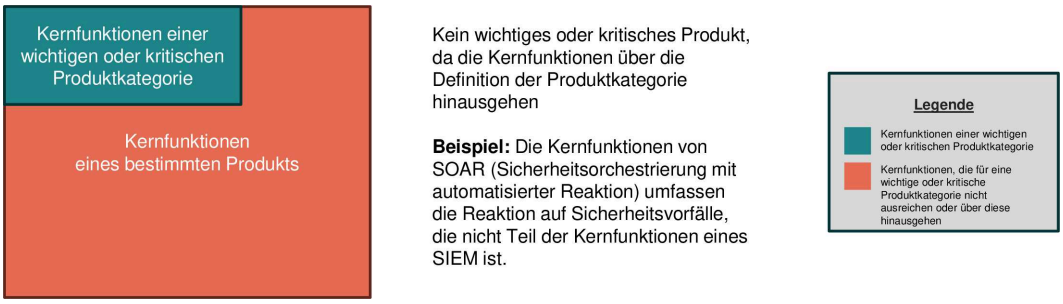
Beispiel 58: Ein Smartphone umfasst ein Betriebssystem, das die in Anhang I Nummer 11 der Durchführungsverordnung (EU) 2025/2392 beschriebene Funktionalität bereitstellt. Während das Betriebssystem die Verwaltung von Hardwareressourcen und die Ausführung von Softwareanwendungen ermöglicht, verfügt das Smartphone als Ganzes über andere Kernfunktionen (beispielsweise jene, den Nutzern die Kommunikation und den Zugang zu Informationen und Diensten zu ermöglichen). Die bloße Integration eines Betriebssystems bedeutet nicht, dass das Smartphone die Kernfunktionen eines Betriebssystems aufweist.

142. Einige Produkte mit digitalen Elementen können einer wichtigen oder kritischen Produktkategorie ähnlich sein oder zu derselben allgemeinen Produktfamilie gehören, aber ihre Kernfunktionen können erheblich über die Kernfunktionen dieser Kategorie hinausgehen oder weit hinter ihnen zurückbleiben. Dies ist nicht der Fall, wenn ein Produkt mit digitalen Elementen zusätzliche Funktionen enthält, die die Kernfunktionen, die ihrerseits denen einer wichtigen oder kritischen Produktkategorie entsprechen, lediglich ergänzen oder verbessern. In diesen Fällen behält das Produkt mit digitalen Elementen die Kernfunktionen dieser Kategorie und wird entsprechend eingestuft. Diese Bewertung sollte sich auf die wichtigsten Merkmale und technischen Fähigkeiten des Produkts stützen, die im Hinblick auf seine Zweckbestimmung objektiv betrachtet werden, und nicht darauf, wie das Produkt mit digitalen Elementen beschrieben oder vermarktet wird, wenn diese Beschreibung nicht die tatsächlichen technischen Merkmale des Produkts wiedergibt.

Beispiel 59: Eine SOAR-Software (Security Orchestration, Automation and Response) kann häufig die Funktionen von Produkten mit digitalen Elementen in der Kategorie „Systeme für die Verwaltung von Sicherheitsinformationen und -ereignissen (SIEM)“ erfüllen, d. h. Daten aus mehreren Quellen sammeln, analysieren und korrelieren und als umsetzbare Informationen für Sicherheitszwecke darstellen. Die Kernfunktionen der Software gehen jedoch erheblich über die eines SIEM hinaus; so gehören Dienste wie die Reaktion auf Sicherheitsvorfälle zu den Kernelementen ihrer technischen Fähigkeiten. Daher wird allgemein davon ausgegangen, dass SOAR-Software nicht die Kernfunktionen von SIEM-Systemen aufweist.

Abbildung 3

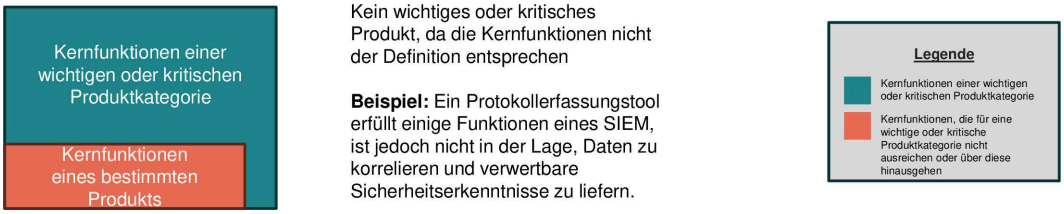
Veranschaulichung der Kernfunktionen eines Produkts mit digitalen Elementen, die erheblich über die Definition einer wichtigen oder kritischen Produktkategorie hinausgehen



Beispiel 60: Bestimmte Protokollerfassungs- und Visualisierungstools sind in der Lage, Protokolldaten zu erfassen und grundlegende Dashboards mit Systemereignissen darzustellen. Diese Tools können zwar Aktivitäten im Bereich der Sicherheitsüberwachung unterstützen, ihre Kernfunktionen bleiben jedoch hinter denen von SIEM-Systemen zurück, da sie weder eine Datenkorrelation durchführen noch verwertbare Sicherheitserkenntnisse liefern. Daher wird bei solchen Tools allgemein nicht davon ausgegangen, dass sie die Kernfunktionen von SIEM-Systemen aufweisen.

Abbildung 4:

Veranschaulichung der Kernfunktionen eines Produkts mit digitalen Elementen, die weit hinter der Definition einer wichtigen oder kritischen Produktkategorie zurückbleiben

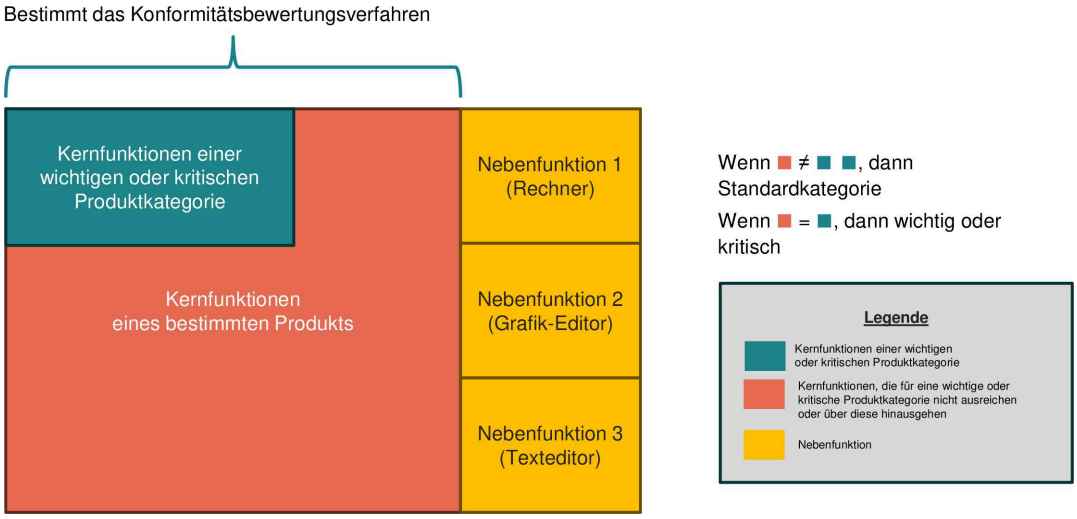


143. Ein Hersteller darf die Kernfunktionen seines Produkts mit digitalen Elementen nicht auf eine Art falsch darstellen, dass er sich damit dem für wichtige oder kritische Produkte mit digitalen Elementen geltenden Konformitätsbewertungsverfahren entzieht, indem er beispielsweise die Rolle bestimmter Funktionen übermäßig betont oder herunterspielt, sodass das Produkt über eine bestimmte Kernfunktion erheblich hinausgeht oder weit hinter ihr zurückbleibt. Dies wäre beispielsweise der Fall, wenn zwischen Werbematerial, Gebrauchsanleitung und der technischen Dokumentation deutliche Unstimmigkeiten bestehen.

144. Ein Produkt mit digitalen Elementen darf für die Zwecke der Bestimmung des anwendbaren Konformitätsbewertungsverfahrens nicht mehr als eine Kernfunktion aufweisen. Gemäß Anhang VII der Cyberresilienzverordnung müssen die Hersteller im Rahmen der technischen Dokumentation die Zweckbestimmung ihres Produkts mit digitalen Elementen und das von ihnen durchgeführte Konformitätsbewertungsverfahren beschreiben. Deshalb sollten die Kernfunktionen des Produkts eindeutig angegeben werden. Dies macht die korrekte Feststellung des anwendbaren Konformitätsbewertungsverfahrens möglich und ermöglicht es den Marktüberwachungsbehörden, die ordnungsgemäße Anwendung der Verordnung zu überwachen und zu überprüfen.

Abbildung 5

Veranschaulichung der Art und Weise, wie sich über die Kernfunktionen eines bestimmten Produkts mit digitalen Elementen die Produktklasse und damit das anzuwendende Konformitätsbewertungsverfahren bestimmen



145. Einige Produkte mit digitalen Elementen werden als Einzelprodukte mit digitalen Elementen in den Verkehr gebracht, bestehen jedoch aus unterschiedlichen Modulen mit separaten Funktionen. Wenn ein Hersteller diese Module auch getrennt auf dem Markt bereitstellt, sodass sie beispielsweise für einen separaten Kauf, eine separate Lizenzierung oder ein separates Abonnement angeboten werden, stellen diese Module eigenständige Produkte mit digitalen Elementen dar. Als solche sind sie auf der Grundlage ihrer jeweiligen Kernfunktionen einzustufen (und unterliegen daher dem jeweiligen Konformitätsbewertungsverfahren auf der Grundlage der Kernfunktionen jedes Moduls). Dies gilt unbeschadet von Modulen, die ausschließlich als Komponenten eines integrierten Produkts mit digitalen Elementen geliefert und nicht getrennt bereitgestellt werden; in solchen Fällen bestimmen sich die Kernfunktionen auf der Ebene des integrierten Produkts mit digitalen Elementen.

Beispiel 61: Ein Hersteller bringt ein Sicherheitspaket in den Verkehr, das mehrere Module umfasst, darunter ein SIEM, ein Angriffserkennungssystem und ein Analysemodul. Der Hersteller bietet für diese Module auch separate Abonnementverträge an. In diesem Szenario ist jedes Modul ein eigenständiges Produkt mit digitalen Elementen und es wird auf der Grundlage seiner eigenen Kernfunktionen klassifiziert. Das SIEM-Modul unterliegt dem Konformitätsbewertungsverfahren für wichtige Produkte mit digitalen Elementen der Klasse I, da seine Kernfunktionen jene von „Systemen für von Sicherheitsinformationen und -ereignissen (SIEM)“ sind. Das Angriffserkennungssystem unterliegt dem Konformitätsbewertungsverfahren für wichtige Produkte mit digitalen Elementen der Klasse II, da seine Kernfunktionen jene von „Firewalls, Angriffserkennungs- und -präventionssystemen“ sind. Das Analysemodul unterliegt dem Konformitätsbewertungsverfahren für „Standard“-Produkte mit digitalen Elementen, da seine Kernfunktionen nicht die einer wichtigen oder kritischen Produktkategorie sind.

146. Bei Nichteinhaltung der in Artikel 32 der Cyberresilienzverordnung festgelegten Pflichten können Geldbußen gemäß Artikel 64 Absatz 3 verhängt werden.

6.2. Konformitätsbewertung für wichtige und kritische Produkte mit digitalen Elementen

147. Sobald der Hersteller die Kernfunktionen seines Produkts mit digitalen Elementen bestimmt hat, muss er eines der anwendbaren Konformitätsbewertungsverfahren durchführen. Der Hersteller muss sicherstellen, dass das Produkt mit digitalen Elementen als Ganzes die grundlegenden Anforderungen erfüllt, wobei gegebenenfalls die Sicherheit der in das Produkt integrierten Komponenten oder Funktionen zu berücksichtigen ist.

148. Ein strengeres Konformitätsbewertungsverfahren unter Beteiligung eines Dritten (auf der Grundlage von Modul B +C, Modul H oder von Schemata für die Cybersicherheitszertifizierung) ist für wichtige Produkte mit digitalen Elementen der Klasse II (mit Ausnahme derer, die gemäß Artikel 32 Absatz 5 als freie und quelloffene Software gelten) und für kritische Produkte mit digitalen Elementen verbindlich vorgeschrieben ([24]). Dagegen müssen wichtige Produkte mit digitalen Elementen der Klasse I (mit Ausnahme derer, die gemäß Artikel 32 Absatz 5 als freie und quelloffene Software gelten) nur dann einem Konformitätsbewertungsverfahren durch Dritte unterzogen werden, wenn der Hersteller einschlägige harmonisierte Normen, deren Fundstellen im *Amtsblatt der Europäischen Union* veröffentlicht wurden (im Folgenden „harmonisierte Normen"), gemeinsame Spezifikationen oder europäische Schemata für die Cybersicherheitszertifizierung mindestens der Vertrauenswürdigkeitsstufe „mittel" nicht oder nur zum Teil angewandt hat ([25]).

149. Damit ein wichtiges Produkt mit digitalen Elementen der Klasse I für das interne Kontrollverfahren infrage kommt, i) müssen daher alle geltenden Anforderungen einer einschlägigen harmonisierten Norm angewandt werden und ii) es muss der Anwendungsbereich der Norm mindestens alle Cybersicherheitsrisiken im Zusammenhang mit den Kernfunktionen dieses Produkts abdecken.

150. Der Anwendungsbereich des Produkts mit digitalen Elementen kann über den in der einschlägigen harmonisierten Norm vorgesehenen Anwendungsbereich hinausgehen, und solche zusätzlichen Funktionen können andere oder zusätzliche Cybersicherheitsrisiken mit sich bringen. Der Hersteller ist stets verpflichtet, eine Risikobewertung gemäß Artikel 13 Absatz 2 durchzuführen, und sollte daher prüfen, ob die Umsetzung einer harmonisierten Norm alle mit dem Produkt mit digitalen Elementen verbundenen Risiken abdeckt. Deckt die Umsetzung der Norm nicht alle Risiken ab, sollte der Hersteller auf andere Weise sicherstellen, dass sein Produkt mit digitalen Elementen den grundlegenden Anforderungen entspricht.

151. Wenn der Hersteller eines wichtigen Produkts mit digitalen Elementen der Klasse I eine einschlägige harmonisierte Norm angewandt hat, die die Risiken im Zusammenhang mit den Kernfunktionen dieses Produkts abdeckt, kann er folglich entscheiden, das interne Kontrollverfahren zum Nachweis der Konformität seines Produkts anzuwenden. Im Rahmen seiner Konformitätsbewertungstätigkeiten muss der Hersteller weiterhin nachweisen, dass alle Risiken, denen sein Produkt mit digitalen Elementen ausgesetzt ist, behandelt werden. Wenn also eine Lücke zwischen der Abdeckung durch die harmonisierte Norm und dem Anwendungsbereich des Produkts mit digitalen Elementen als Ganzes besteht, muss der Hersteller nach wie vor dokumentieren, welche zusätzlichen Maßnahmen bei ihm vorhanden sind, um diese Risiken zu behandeln.

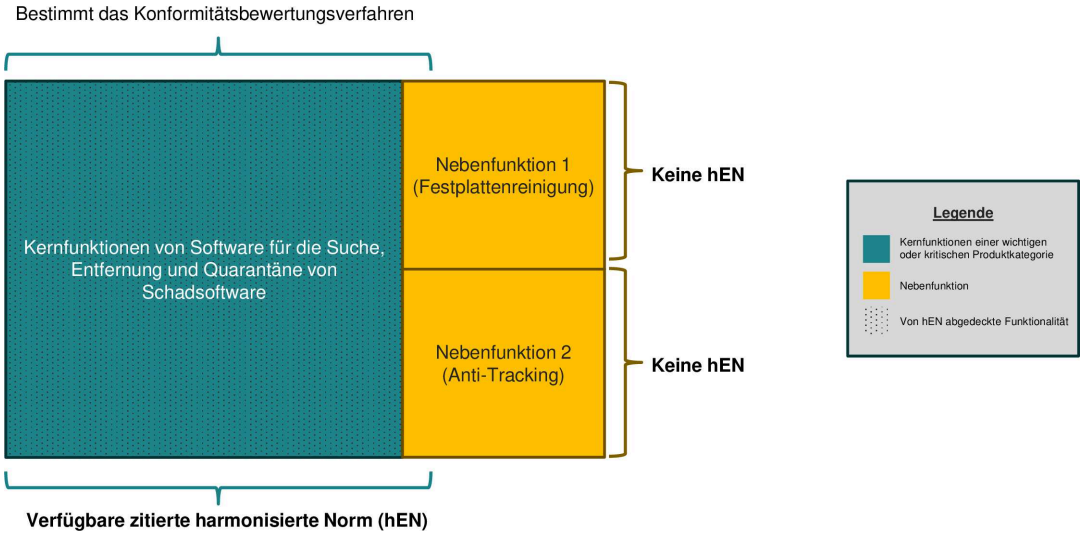
Beispiel 62: Eine Antivirensoftware verfügt gemäß Anhang I Nummer 4 der Durchführungsverordnung (EU) 2025/2392 über die Kernfunktion einer Software, die nach Schadsoftware sucht, diese entfernt oder in Quarantäne stellt. Dieses Produkt mit digitalen Elementen enthält ferner zusätzliche Funktionen, nämlich eine Festplattenreinigungsfunktion und eine Anti-Tracking-Funktion, die den Nutzer beim Navigieren im Internet schützt. Der Hersteller führt eine Risikobewertung durch, die sich auf das Produkt mit digitalen Elementen in seiner Gesamtheit erstreckt, einschließlich der Kernfunktion des Antivirenprogramms, der Festplattenreinigungsfunktion und der Anti-Tracking-Funktion. Er wendet eine harmonisierte Norm an, die die Risiken im Zusammenhang mit der Kernfunktion des Antivirenprogramms abdeckt, sowie zusätzliche Maßnahmen zum Umgang mit Risiken, die sich aus zusätzlichen Funktionen ergeben. Dem Hersteller ist es gestattet, für seine Konformitätsbewertung das interne Kontrollverfahren anzuwenden, das das Produkt mit digitalen Elementen als Ganzes abdeckt, einschließlich der Festplattenreinigungs- und der Anti-Tracking-Funktion.

([24]) Dies ist auch der Fall, wenn ein europäisches Schema für die Cybersicherheitszertifizierung mindestens der Vertrauenswürdigkeitsstufe „mittel" angewandt wird, da die Einbeziehung einer externen Zertifizierungsstelle erforderlich ist.

([25]) Im Interesse einer möglichst knappen Darstellung bezieht sich der Rest dieses Abschnitts nur auf harmonisierte Normen, deren Fundstellen im *Amtsblatt der Europäischen Union* veröffentlicht wurden. Dieselben Leitlinien gelten jedoch auch für gemeinsame Spezifikationen, die gemäß Artikel 27 Absatz 2 angenommen wurden, und für europäische Schemata für die Cybersicherheitszertifizierung, wenn sie von der Kommission im Wege delegierter Rechtsakte gemäß Artikel 27 Absatz 9 festgelegt wurden.

Abbildung 6

Veranschaulichung der Art und Weise, in der sich über die Verwendung einer zitierten harmonisierten Norm, die nur Kernfunktionen abdeckt, das anzuwendende Konformitätsbewertungsverfahren bestimmt



152. Dies ist auch der Fall, wenn das Produkt mit digitalen Elementen eine zusätzliche Funktion enthält, die selbst jene eines anderen wichtigen oder kritischen Produkts mit digitalen Elementen ist. Tatsächlich wird durch die Kernfunktion des Produkts mit digitalen Elementen als Ganzes und nicht durch die Funktion der isoliert betrachteten integrierten Komponenten bestimmt, ob das Produkt mit digitalen Elementen zur wichtigen oder kritischen Produktkategorie gehört (und damit dem geltenden Konformitätsbewertungsverfahren unterliegt). Wenn beispielsweise ein Produkt mit digitalen Elementen die Kernfunktion eines wichtigen Produkts mit digitalen Elementen der Klasse I aufweist, unterliegt dieses Produkt als Ganzes dem Konformitätsbewertungsverfahren, das für wichtige Produkte mit digitalen Elementen der Klasse I gilt, auch wenn es eine Komponente enthält, die selbst ein kritisches Produkt mit digitalen Elementen ist. In diesen Fällen ist es dem Hersteller bei Anwendung einer harmonisierten Norm, die die Risiken im Zusammenhang mit der Kernfunktion dieses Produkts abdeckt, gestattet, das interne Kontrollverfahren anzuwenden.

Beispiel 63: Ein Hardwareprodukt mit digitalen Elementen weist die Kernfunktionen eines Routers gemäß Anhang I Nummer 12 der Durchführungsverordnung (EU) 2025/2392 auf. Dieses Produkt mit digitalen Elementen umfasst ferner zusätzliche Funktionen, darunter eine Firewalling-Funktion, da es eine Firewall-Komponente enthält. Der Hersteller führt eine Risikobewertung durch, die sich auf das Produkt mit digitalen Elementen in seiner Gesamtheit erstreckt, einschließlich der Kernfunktionen des Routers und der Firewall-Funktionalität. Er wendet eine harmonisierte Norm an, die die Risiken im Zusammenhang mit den Kernfunktionen des Routers abdeckt, sowie zusätzliche Maßnahmen zum Umgang mit Risiken, die sich aus zusätzlichen Funktionen ergeben. So kann der Hersteller beispielsweise die harmonisierte Norm für Firewalls anwenden, um die mit der Firewall-Funktionalität verbundenen Risiken abzudecken. Dem Hersteller ist es gestattet, für seine Konformitätsbewertung das interne Kontrollverfahren anzuwenden, das das Produkt mit digitalen Elementen als Ganzes abdeckt, einschließlich der Firewall-Funktionalität.

6.3. Auswirkungen auf die Konformitätsvermutung

153. In Artikel 27 Absatz 1 der Cyberresilienzverordnung ist festgelegt, dass bei Produkten mit digitalen Elementen und vom Hersteller festgelegten Verfahren, die mit harmonisierten Normen oder Teilen davon übereinstimmen, deren Fundstellen im *Amtsblatt der Europäischen Union* veröffentlicht worden sind, eine Konformität mit den grundlegenden Cybersicherheitsanforderungen der Cyberresilienzverordnung vermutet wird, die von den betreffenden Normen oder Teilen davon abgedeckt sind ([26]). Mit Artikel 27 Absatz 5 wird dieselbe Konformitäts-

([26]) In Abschnitt 4.1.2.2 des „Blue Guide“ heißt es eindeutig: „Bei risikobezogenen Harmonisierungsrechtsvorschriften … [trägt der] Hersteller auch dann, wenn sie harmonisierte Normen anwenden, deren Fundstellen im *Amtsblatt der Europäischen Union* in Kraf veröffentlicht sind, die alleinige Verantwortung für die Beurteilung aller mit ihrem Produkt verbundenen Risiken und [muss] daher bestimmen …, welche der wesentlichen (oder sonstigen) Anforderungen einschlägig sind. Nach dieser Beurteilung kann sich der Hersteller für die Anwendung von technischen Spezifikationen aus harmonisierten Normen, deren Fundstellen im *Amtsblatt der Europäischen Union* in Kraf veröffentlicht sind, entscheiden, um ‚Maßnahmen zur Risikominderung‘ umzusetzen, die in den harmonisierten Normen festgelegt sind.“

vermutung auf Produkte mit digitalen Elementen und vom Hersteller festgelegte Verfahren ausgeweitet, die den von der Kommission im Wege von Durchführungsrechtsakten angenommenen gemeinsamen Spezifikationen entsprechen, und in Artikel 27 Absatz 8 ist die Konformitätsvermutung für Produkte mit digitalen Elementen und vom Hersteller festgelegte Verfahren vorgesehen, für die im Rahmen eines gemäß der Verordnung (EU) 2019/881 angenommenen europäischen Schemas für die Cybersicherheitszertifizierung eine EU-Konformitätserklärung oder ein EU-Zertifikat ausgestellt wurde, sofern dies durch delegierte Rechtsakte gemäß Artikel 27 Absatz 9 festgelegt wurde ([27]).

154. Wenn der Hersteller eine harmonisierte Norm angewandt hat, deren Fundstellen im *Amtsblatt der Europäischen Union* veröffentlicht wurden, gilt daher für ihn hinsichtlich der von dieser Norm abgedeckten Risiken die Konformitätsvermutung. Dies könnte beispielsweise der Fall sein, wenn die betreffende harmonisierte Norm alle Risiken im Zusammenhang mit den Kernfunktionen eines Produkts mit digitalen Elementen abdeckt und es keine zusätzlichen Funktionen gibt, die Cybersicherheitsrisiken aufweisen. So wird beispielsweise davon ausgegangen, dass die harmonisierte Norm für Router zumindest die Risiken im Zusammenhang mit den Kernfunktionen dieser Produkte mit digitalen Elementen abdecken wird. Wenn ein solches Produkt keine zusätzlichen Funktionen enthält oder wenn diese zusätzlichen Funktionen keine Risiken aufweisen, die in der Norm nicht berücksichtigt sind, kann für das Produkt mit digitalen Elementen die Konformitätsvermutung gelten.

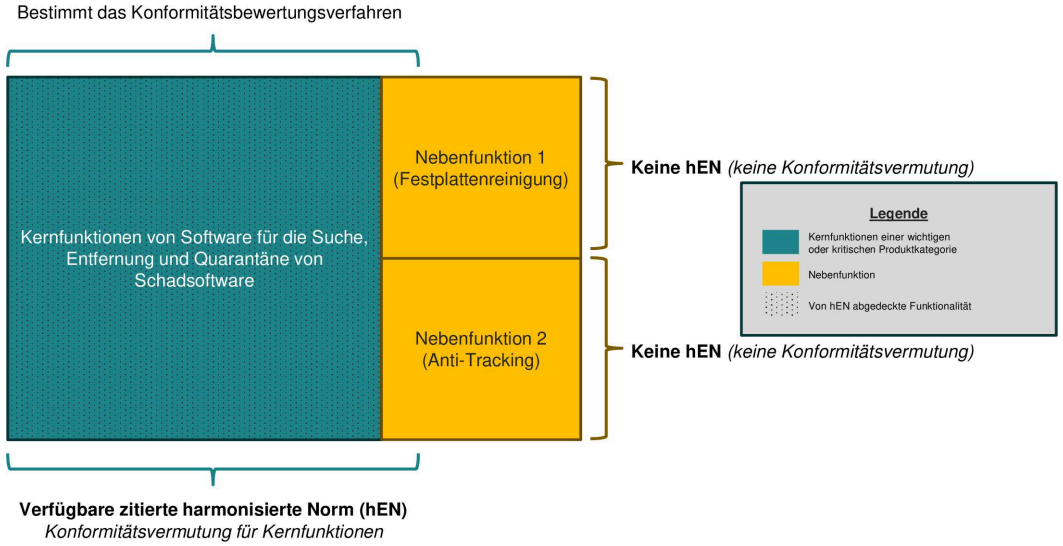
155. In den unter den Randnummern 151 und 152 erörterten Fällen ist es dem Hersteller gestattet, das interne Kontrollverfahren anzuwenden, da die harmonisierte Norm die Risiken abdeckt, die mit den Kernfunktionen des Produkts mit digitalen Elementen einhergehen. Die in diesen Beispielen beschriebenen Produkte mit digitalen Elementen können jedoch über den Anwendungsbereich der harmonisierten Normen hinausgehen, und zusätzliche Funktionen können Cybersicherheitsrisiken aufweisen, die von einer solchen harmonisierten Norm nicht erfasst sind. Für diese zusätzlichen Funktionen dieser Produkte mit digitalen Elementen gilt die Konformitätsvermutung daher möglicherweise nicht.

Beispiel 64: Eine Antivirensoftware verfügt über die Kernfunktionen einer Software, die nach Schadsoftware sucht, diese entfernt oder in Quarantäne stellt, und die mit diesen Kernfunktionen verbundenen Risiken sind von der harmonisierten Norm abgedeckt. Dieses Produkt mit digitalen Elementen enthält ferner zusätzliche Funktionen, nämlich eine Festplattenreinigungsfunktion und eine Anti-Tracking-Funktion, die den Nutzer beim Navigieren im Internet und damit vor Risiken schützt, die nicht durch die harmonisierte Norm abgedeckt sind. Wird die harmonisierte Norm angewandt, so ist es dem Hersteller gestattet, für seine Konformitätsbewertung das interne Kontrollverfahren zu nutzen. Für ihn gilt die Konformitätsvermutung in Bezug auf die Risiken im Zusammenhang mit den Kernfunktionen dieses Produkts, nicht aber in Bezug auf die Risiken, die mit zusätzlichen Funktionen verbunden sind.

([27]) Wie weiter oben, bezieht sich der Rest dieses Abschnitts im Interesse einer möglichst knappen Darstellung nur auf harmonisierte Normen, deren Fundstellen im *Amtsblatt der Europäischen Union* veröffentlicht wurden. Dieselben Leitlinien gelten jedoch auch für gemeinsame Spezifikationen und für europäische Schemata für die Cybersicherheitszertifizierung.

Abbildung 7

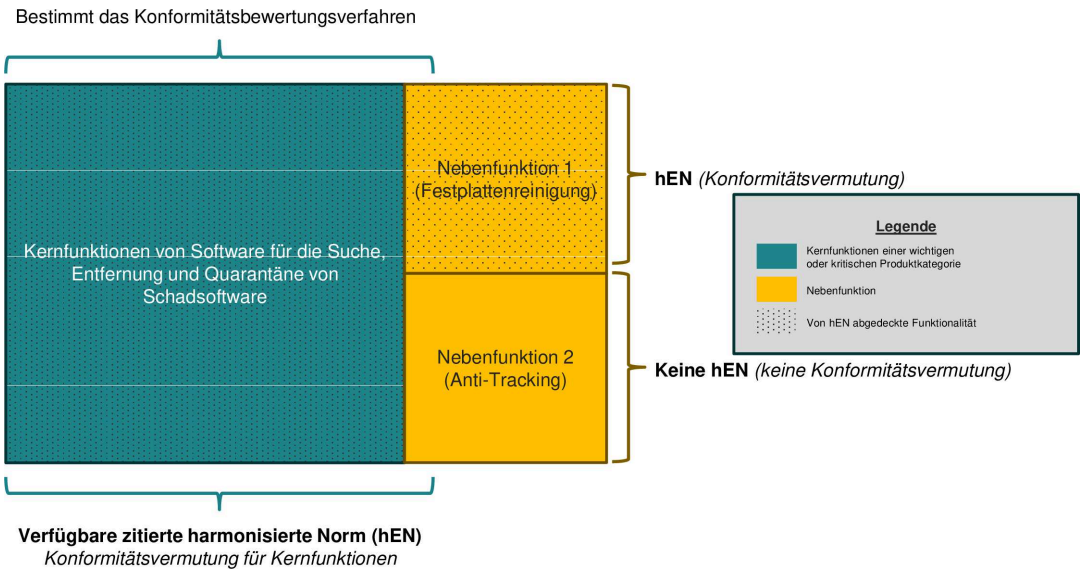
Aufgrund der harmonisierten Norm gilt für die Kernfunktion die Konformitätsvermutung, da die Norm alle Risiken im Zusammenhang mit diesen Kernfunktionen abdeckt; für Nebenfunktionen gilt diese Vermutung hingegen nicht.



Beispiel 65: In demselben Szenario wie im vorherigen Beispiel wurde die harmonisierte Norm nun aktualisiert, sodass sie auch Risiken im Zusammenhang mit einer der zusätzlichen Funktionen abdeckt, nämlich der Festplattenreinigungsfunktion, nicht aber im Zusammenhang mit der anderen zusätzlichen Funktion (d. h. der Anti-Tracking-Funktion). Wird die harmonisierte Norm angewandt, so ist es dem Hersteller gestattet, für seine Konformitätsbewertung das interne Kontrollverfahren zu nutzen. Für ihn gilt eine Konformitätsvermutung in Bezug auf die Risiken im Zusammenhang mit den Kernfunktionen dieses Produkts und der Festplattenreinigungsfunktion, nicht aber in Bezug auf die Risiken im Zusammenhang mit der Anti-Tracking-Funktion.

Abbildung 8

Aufgrund der harmonisierten Norm gilt für die Kernfunktionen und die Nebenfunktion 1 die Konformitätsvermutung, da die Norm alle mit diesen beiden Funktionen verbundenen Risiken abdeckt; für die Nebenfunktion 2 gilt diese Vermutung hingegen nicht.



7. BEWERTUNG DER CYBERSICHERHEITSRISIKEN UND INTEGRATION VON PRODUKTEN MIT DIGITALEN ELEMENTEN UND KOMPONENTEN

7.1. Zur Bewertung und Behandlung von Cybersicherheitsrisiken

156. Bei der Bewertung der Cybersicherheitsrisiken gemäß Artikel 13 Absatz 2 der Cyberresilienzverordnung müssen die Hersteller relevante Risiken ermitteln und deren potenzielle Auswirkungen auf das Produkt mit digitalen Elementen bewerten. Die Hersteller müssen auch geeignete Maßnahmen umsetzen, um diesen Risiken im Einklang mit den grundlegenden Anforderungen in Anhang I zu begegnen.

157. Beim organisatorischen Risikomanagement werden die Risiken in der Regel anhand von Akzeptanzkriterien bewertet, denen die internen Ziele oder die Risikobereitschaft der Organisation zugrunde liegen. Im Gegensatz dazu sollte im Rahmen der Cyberresilienzverordnung das verbleibende Cybersicherheitsrisiko vor dem Hintergrund der Anforderung bewertet werden, dass das in den Verkehr gebrachte Produkt mit digitalen Elementen unter Berücksichtigung seiner Zweckbestimmung und seiner vernünftigerweise vorhersehbaren Verwendung auf der Grundlage der Risiken ein angemessenes Cybersicherheitsniveau gewährleistet.

158. Dementsprechend sind die interne Risikotoleranz, die Geschäftsstrategie oder reine Kostenerwägungen des Herstellers für die Feststellung, ob Risiken begegnet wurde, nicht relevant. Für die Zwecke des Artikels 13 Absätze 2 und 3 müssen die Hersteller in der Lage sein, unter Berücksichtigung der Zweckbestimmung, der vernünftigerweise vorhersehbaren Verwendung und der Verwendungsbedingungen, gegebenenfalls einschließlich der Betriebsumgebung (beispielsweise der vorgesehenen Nutzer des Produkts mit digitalen Elementen) und der zu schützenden Anlagen, sowie unter Berücksichtigung der voraussichtlichen Nutzungsdauer des Produkts mit digitalen Elementen festzustellen, ob den ermittelten Cybersicherheitsrisiken durch die Umsetzung der grundlegenden Anforderungen in Anhang I Teil I ausreichend begegnet wurde.

159. Das verbleibende Cybersicherheitsrisiko ist ein inhärentes Ergebnis der Risikobewertung und -behandlung. Es wird anerkannt, dass sich Cybersicherheitsrisiken in der Praxis nicht vollständig beseitigen lassen. Dass Restrisiken bestehen, bedeutet jedoch nicht, dass nach dem Ermessen des Herstellers jedes Risiko akzeptiert werden kann. Ein Produkt mit digitalen Elementen darf nur in den Verkehr gebracht werden, wenn den Restrisiken, sobald geeignete Maßnahmen ergriffen wurden, durch die Umsetzung der grundlegenden Anforderungen unter Berücksichtigung der Zweckbestimmung und der vernünftigerweise vorhersehbaren Verwendung des Produkts mit digitalen Elementen ausreichend begegnet wurde.

160. Werden Cybersicherheitsrisiken festgestellt, so sind die Hersteller gemäß Artikel 13 Absatz 3 verpflichtet, diese durch geeignete Maßnahmen, auch auf Produktebene, anzugehen. Je nach den Umständen kann dies beispielsweise die Verringerung der Angriffsfläche, die Umsetzung technischer Schutzvorkehrungen, die Einschränkung oder Anpassung der Funktionalität oder die genauere Definition der Zweckbestimmung des Produkts mit digitalen Elementen umfassen. Die Hersteller können auch Schritte unternehmen, um die vernünftigerweise vorhersehbare Verwendung des Produkts mit digitalen Elementen zu gestalten, beispielsweise durch Risikokommunikation, Benutzerleitfäden oder über die Konzeption der Benutzeroberfläche, um das Nutzerverhalten hin zu sicheren Nutzungsmustern zu lenken.

161. Die Cyberresilienzverordnung sieht nicht vor, dass Cybersicherheitsrisiken oder -verantwortung auf Nutzer oder Dritte übertragen werden, um Mängel bei der Produktkonzeption auszugleichen oder um zu rechtfertigen, dass Cybersicherheitsrisiken nicht begegnet wird. Die Verpflichtung, ein sicheres Produkt mit digitalen Elementen in den Verkehr zu bringen und Konformität mit den grundlegenden Anforderungen nachzuweisen, verbleibt beim Hersteller.

162. Informationen und Anweisungen, die den Nutzern zur Verfügung gestellt werden, können dazu eingesetzt werden, die sichere Einführung und den sicheren Betrieb des Produkts mit digitalen Elementen zu unterstützen, auch dann, wenn sich der Hersteller dafür entschieden hat, die Zweckbestimmung dieses Produkts auf vertrauenswürdige Umgebungen zu beschränken, und die Nutzer in einer Weise über Restrisiken zu informieren, die der Art des Produkts mit digitalen Elementen und seinen vorgesehenen Nutzern angemessen ist.

Beispiel 66: Ein Hersteller entwickelt einen Industriesensor zur Verwendung in vertrauenswürdigen Umgebungen. Um die ordnungsgemäße Funktionalität des Sensors nicht zu beeinträchtigen, setzt der Hersteller keine Maßnahmen zum Schutz vor physischen Angriffen auf den Sensor selbst um. Zur Minderung der in der Risikobewertung ermittelten Risiken beschränkt der Hersteller die Zweckbestimmung des Sensors auf die Verwendung in vertrauenswürdigen Umgebungen, in denen ein unbefugter physischer Zugang zum Produkt mit digitalen Elementen nicht möglich ist. Die Informationen und Anweisungen für die Nutzer enthalten klare Informationen zu diesen Einschränkungen für die Verwendung des Sensors – in einer Weise, die der Art des Produkts mit digitalen Elementen und mit Blick auf die vorgesehenen Nutzer angemessen ist.

Beispiel 67: Ein Hersteller entwickelt eine Softwareanwendung für den professionellen Einsatz auf verwalteten Desktop-Computern und mobilen Geräten. Die Anwendung verarbeitet lokal gespeicherte sensible Daten und nutzergenerierte Inhalte. Bei der Risikobewertung ermittelt der Hersteller das Risiko eines unbefugten Zugriffs auf diese Daten, wenn sie in Klartext auf dem Gerät gespeichert sind. Anstatt einen proprietären Verschlüsselungsmechanismus innerhalb der Anwendung selbst zu konzipieren und implementieren, entscheidet sich der Hersteller dafür, auf die Verschlüsselungs- und Schlüsselverwaltungsfunktionen zu setzen, die von dem Betriebssystem, auf dem die Anwendung betrieben werden soll, bereitgestellt werden, da die integrierten kryptografischen Dienste des Betriebssystems ausgereift sind und regelmäßig gewartet werden.

163. Werden bei der Bewertung der Cybersicherheitsrisiken Risiken ermittelt, denen durch geeignete Maßnahmen nicht angemessen begegnet werden kann, können zur Einhaltung der Cyberresilienzverordnung Änderungen der Konzeption, der Funktion oder der Zweckbestimmung des Produkts mit digitalen Elementen erforderlich sein. Erwägungen, die sich ausschließlich auf die Kosten oder die wirtschaftliche Machbarkeit beziehen, stellen keinen ausreichenden Grund dafür dar, solche Risiken unberücksichtigt zu lassen, wenn dies verhindern würde, dass das Produkt mit digitalen Elementen die grundlegenden Anforderungen erfüllt.

7.2. Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen, sodass angesichts der Risiken ein angemessenes Maß an Cybersicherheit gewährleistet ist

164. Die in Anhang I Teil I Nummer 1 der Cyberresilienzverordnung genannte grundlegende Cybersicherheitsanforderung sieht vor, dass Produkte mit digitalen Elementen so konzipiert, entwickelt und hergestellt werden, dass sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten.

165. Mit dieser grundlegenden Anforderung soll allen Cybersicherheitsrisiken begegnet werden, die im Rahmen der Bewertung der Cybersicherheitsrisiken ermittelt wurden. Dies umfasst insbesondere Cybersicherheitsrisiken, die im Rahmen der Umsetzung der grundlegenden Anforderungen in Anhang I Teil I mit Ausnahme von Nummer 1 nicht anderweitig angemessen angegangen werden. Diese grundlegenden Anforderungen unterscheiden sich von der rechtlichen Verpflichtung zur Durchführung einer Bewertung der Cybersicherheitsrisiken, die gemäß Artikel 13 Absatz 2 durchzuführen ist.

166. Werden alle relevanten Cybersicherheitsrisiken im Zusammenhang mit einem Produkt mit digitalen Elementen behandelt, indem geeignete Maßnahmen zur Erfüllung der geltenden grundlegenden Anforderungen mit Ausnahme von Nummer 1 umgesetzt werden, so gilt die in Anhang I Teil I Nummer 1 genannte grundlegende Anforderung als erfüllt. Werden hingegen bei der Bewertung der Cybersicherheitsrisiken zusätzliche Risiken festgestellt, denen durch solche Maßnahmen nicht vollständig begegnet wird, sind die Hersteller verpflichtet, geeignete Maßnahmen in Bezug auf das Produkt mit digitalen Elementen zu ergreifen, um diesen Risiken entgegenzuwirken, sodass sie die in Anhang I Teil I Nummer 1 genannte grundlegende Anforderung erfüllen. In der Praxis wird in den meisten Fällen erwartet, dass die Einhaltung der anderen grundlegenden Anforderungen zur Einhaltung dieser Anforderung führt.

7.3. Risikobewertung und Sorgfaltspflicht in Bezug auf externe Abhängigkeiten und integrierte Komponenten

167. Mit der Cyberresilienzverordnung werden zwei unterschiedliche, einander jedoch ergänzende Pflichten für Hersteller in Bezug auf das Cybersicherheitsrisikomanagement festgelegt. Erstens sind die Hersteller nach Artikel 13 Absatz 2 verpflichtet, eine Bewertung der Cybersicherheitsrisiken für das Produkt mit digitalen Elementen selbst durchzuführen. Zweitens wird ihnen durch Artikel 13 Absatz 5 die Sorgfaltspflicht in Bezug auf integrierte Komponenten auferlegt. Gemeinsam sollen diese beiden Verpflichtungen sicherstellen, dass das Produkt mit digitalen Elementen sicher bleibt, auch wenn es auf Datenfernverarbeitungslösungen, Ferndiensten oder Software- oder Hardwarekomponenten Dritter beruht.

168. Die Bewertung der Cybersicherheitsrisiken betrifft die Ermittlung und das Management relevanter Risiken, die sich auf das Produkt mit digitalen Elementen auswirken können, einschließlich Risiken, die außerhalb des Produkts selbst entstehen, wie externe Netze, Umweltfaktoren oder andere externe Aspekte, die sich auf das Produkt mit digitalen Elementen auswirken könnten oder auf denen das Produkt beruht. In Bezug auf solche externen Risiken enthält die Cyberresilienzverordnung keine Bestimmung, der zufolge die Hersteller verpflichtet sind, das externe Umfeld zu verwalten oder zu steuern. Vielmehr sind die Hersteller verpflichtet, solche Risiken zu ermitteln und sie durch die Konzeption und Entwicklung des Produkts mit digitalen Elementen selbst zu mindern. Dies umfasst die Umsetzung der entsprechenden grundlegenden Anforderungen in Anhang I Teil I und erforderlichenfalls die Bereitstellung von Informationen und Anweisungen zu Integrations- oder Einsatzrisiken für die Nutzer.

169. So kann es sein, dass ein Hersteller beispielsweise das Risiko ermittelt, dass Unbefugte während des Betriebs des Produkts Zugang zu Back-End-Systemen erhalten, die nicht Teil des Produkts mit digitalen Elementen selbst sind, und versuchen, böswillige Befehle an das Produkt mit digitalen Elementen zu senden. Solche Back-End-Systeme stellen keine Datenfernverarbeitungslösungen dar und fallen daher für die Zwecke der Cyberresilienzverordnung nicht in den Anwendungsbereich des Produkts mit digitalen Elementen, wenn sie nicht vom Hersteller oder unter seiner Verantwortung konzipiert und entwickelt werden oder wenn sie keine der Funktionen des Produkts mit digitalen Elementen unterstützen. Dennoch verpflichtet die Cyberresilienzverordnung den Hersteller, dem von ihnen möglicherweise ausgehenden Risiko durch Maßnahmen auf Produktebene zu begegnen, beispielsweise durch die Anforderung einer kryptografischen Authentifizierung von Fernbefehlen, die Überprüfung der Integrität von Konfigurationsänderungen oder die Generierung sicherheitsrelevanter Protokolle oder Warnungen, wenn ungewöhnliches Verhalten festgestellt wird. Ebenso ist es möglich, dass, wenn ein Hersteller ein Risiko feststellt, das sich aus der Nichtverfügbarkeit eines solchen externen Dienstes ergibt, beispielsweise aufgrund von Stromausfällen oder Ausfällen der Infrastruktur, gemäß der Cyberresilienzverordnung Risikominderungsmaßnahmen gegen solche Cybersicherheitsrisiken auf Produktebene umgesetzt werden müssen, zum Beispiel, um sicherzustellen, dass der Ausfall nicht dazu führt, dass das Produkt mit digitalen Elementen in einen unsicheren Zustand gerät. In solchen Fällen ist in der Cyberresilienzverordnung geregelt, wie das Produkt mit digitalen Elementen auf solche externen Risiken reagiert; sie schreibt jedoch weder vor, wie die Back-End-Infrastruktur organisiert, mit Personal ausgestattet oder betrieben wird, noch wird darin diese Infrastruktur als Teil des Produkts mit digitalen Elementen behandelt.

170. Die Sorgfaltspflicht bezieht sich auf Elemente, die Teil des Produkts mit digitalen Elementen selbst sind, insbesondere integrierte Software- oder Hardwarekomponenten, die von Dritten bereitgestellt werden. Die Hersteller sind verpflichtet, geeignete Maßnahmen zu ergreifen, damit solche Komponenten der Konformität des Produkts mit digitalen Elementen mit den grundlegenden Anforderungen nicht zuwiderlaufen. Dies lässt sich nur erreichen, indem festgelegt wird, welche Anforderungen die Komponenten des Produkts mit digitalen Elementen erfüllen müssen, damit die in Bezug auf das Produkt bestehenden Cybersicherheitsziele erreicht werden, und indem auf risikobasierte Weise überprüft wird, ob diese Komponenten den Bedürfnissen des Produkts entsprechen, wie es auch in Erwägungsgrund 34 dargelegt ist.

171. Im Einklang mit der Bewertung der Cybersicherheitsrisiken muss der Hersteller die Anforderungen ermitteln, die die integrierte Komponente erfüllen sollte. Stützt sich das Produkt mit digitalen Elementen beispielsweise auf kryptografische Funktionen, Aktualisierungsmechanismen oder sichere Kommunikation, die von einer Komponente bereitgestellt werden, so muss der Hersteller im Rahmen seiner Sorgfaltspflicht diese Bedürfnisse ermitteln und überprüfen, ob die Komponente sie erfüllt. Der zu diesem Zweck zu erbringende Nachweis kann in Form von Unterlagen des Komponentenherstellers vorgelegt werden, beispielsweise technischen Spezifikationen, Sicherheitsunterlagen oder einschlägigen Konformitäts- oder Gewährleistungsunterlagen. Gegebenenfalls kann der Hersteller auch Prüfungen durchführen, um festzustellen, ob diese Komponenten die einschlägigen Funktionen angemessen erfüllen. Die Sorgfaltspflicht ist zwar eine gesonderte rechtliche Verpflichtung, unterstützt und untermauert jedoch die Fähigkeit des Herstellers, die Einhaltung der grundlegenden Anforderungen an das Produkt mit digitalen Elementen als Ganzes nachzuweisen.

172. Im Rahmen der Bewertung der Risiken für das Produkt mit digitalen Elementen als Ganzes müssen Elemente außerhalb des Produkts, wie Umweltelemente, externe Infrastruktur, andere Systeme oder Netze, bei der Bewertung der Cybersicherheitsrisiken berücksichtigt und gegebenenfalls durch Maßnahmen auf Produktebene angegangen werden, damit sichergestellt ist, dass das Produkt mit digitalen Elementen den grundlegenden Anforderungen entspricht. Komponenten, die physisch oder logisch in das Produkt mit digitalen Elementen integriert sind, aber von Dritten bezogen werden, müssen ebenfalls in die Risikobewertung einbezogen werden. Für die Zwecke der Konformität sollte der Hersteller solche Komponenten jedoch als extern gelieferte Bauteile behandeln, deren Eigenschaften bei der Integration im Rahmen der Sorgfaltspflicht überprüft werden, da der Hersteller sie möglicherweise nicht umgestaltet oder neu entwickelt hat.

173. Die gleiche Logik gilt für die Entwicklung und Integration von Komponenten. Entwickelt der Hersteller selbst Funktionen, so muss er die grundlegenden Anforderungen direkt umsetzen. Wenn der Hersteller von anderen entwickelte Komponenten integriert, muss er mit der gebotenen Sorgfalt sicherstellen, dass diese Komponenten so verwendet werden können, dass das Produkt mit digitalen Elementen als Ganzes die Anforderungen erfüllt. In beiden Fällen ist das Ziel dasselbe: Das Produkt mit digitalen Elementen soll in der in den Verkehr gebrachten Form ein angemessenes Cybersicherheitsniveau gemäß den Anforderungen der Cyberresilienzverordnung erreichen, wobei die in der Bewertung der Cybersicherheitsrisiken ermittelten Risiken zu berücksichtigen sind.

7.4. **Wiederverwendung von Risikobewertungs- und Konformitätsunterlagen für Familien von Produkten mit digitalen Elementen**

174. Die Hersteller können Produkte mit ähnlichen digitalen Elementen in den Verkehr bringen, beispielsweise verschiedene Varianten, Modelle oder Konfigurationen derselben Produktfamilie. Wenn solche Produkte mit digitalen Elementen dieselbe Architektur, dieselbe sicherheitsrelevante Konzeption und dieselbe Zweckbestimmung aufweisen und denselben Cybersicherheitsrisiken ausgesetzt sind, sind die Hersteller gemäß der Cyberresilienzverordnung nicht verpflichtet, für die Zwecke der Risikobewertung und der Konformitätsbewertung jede Variante als gänzlich eigenständiges Produkt mit digitalen Elementen zu behandeln.

175. In solchen Fällen können sich die Hersteller, sofern alle betroffenen Varianten im Hinblick auf die einschlägigen Risiken und grundlegenden Anforderungen angemessen abgedeckt sind, auf Folgendes stützen: i) eine einzige Bewertung der Cybersicherheitsrisiken, die gemäß Artikel 13 Absatz 2 der Cyberresilienzverordnung durchgeführt wird; ii) einen einzelnen Satz technischer Unterlagen und iii) ein einziges Konformitätsbewertungsverfahren. Dies ermöglicht auch, eine einzige EU-Konformitätserklärung für die Gruppe von Produkten mit digitalen Elementen auszustellen, sofern darin die Produktvarianten, für die sie gilt, eindeutig angegeben sind.

176. Entscheidend ist, ob die Unterschiede zwischen den Varianten für die Cybersicherheit relevant sind. Bei Änderungen, die sich nicht auf die Cybersicherheitsmerkmale des Produkts mit digitalen Elementen auswirken, wie Unterschiede in der Farbe, dem Formfaktor, der Speichergröße oder in Bezug auf andere nicht sicherheitsrelevante Merkmale, sind keine separaten Risikobewertungen oder Konformitätsbewertungen erforderlich. Umgekehrt können sich in einigen Fällen Varianten in einer Weise unterscheiden, die sich auf die Umsetzung wesentlicher Anforderungen auswirkt, beispielsweise durch verschiedene Kommunikationsschnittstellen, Software-Stacks, Aktualisierungsmechanismen oder Fernkonnektivität. In solchen Fällen müssen diese Unterschiede in der Risikobewertung und erforderlichenfalls aus der Konformitätsbewertung und der technischen Dokumentation hervorgehen.

177. Die Hersteller bleiben dafür verantwortlich, dass die Risikobewertung und die zugehörige Dokumentation die in den Verkehr gebrachten Produkte mit digitalen Elementen exakt wiedergeben. Wenn eine neue Variante neue Cybersicherheitsrisiken mit sich bringt oder die Art und Weise der Umsetzung grundlegender Anforderungen ändert, müssen die bestehende Risikobewertung und die Konformitätsdokumentation entsprechend aktualisiert werden. Eine einzige Konformitätsbewertung ist nur dann ausreichend, wenn die Produkte mit digitalen Elementen in Bezug auf ihre Cybersicherheitsmerkmale keine Unterschiede aufweisen.

8. **DATENFERNVERARBEITUNG**

178. In Artikel 3 Nummer 1 der Cyberresilienzverordnung ist ein Produkt mit digitalen Elementen definiert als „ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in den Verkehr gebracht werden“. Vor diesem Hintergrund muss der Hersteller das Produkt mit digitalen Elementen als Ganzes betrachten, einschließlich seiner Datenfernverarbeitungslösungen. Wenn beispielsweise nachgewiesen wird, dass das Produkt mit digitalen Elementen den grundlegenden Anforderungen von Anhang I entspricht, müssen Datenfernverarbeitungslösungen berücksichtigt werden, beginnend mit der Risikobewertung (Artikel 13 Absatz 2). Gleiches gilt für Lebenszyklusverpflichtungen wie der Meldung aktiv ausgenutzter Schwachstellen und schwerwiegender Sicherheitsvorfälle (Artikel 14).

179. Zweck der vorliegenden Leitlinien ist es, den Herstellern weitere Unterstützung bei der Feststellung zu bieten, ob ihr Produkt mit digitalen Elementen über Datenfernverarbeitungslösungen gemäß der Definition in der Cyberresilienzverordnung verfügt und wie sie ihre diesbezüglichen Konformitätspflichten erfüllen können. In den vorliegenden Leitlinien werden zunächst die Begriffsbestimmungen und Erwägungsgründe der Cyberresilienzverordnung analysiert und in der Folge eine Reihe von Fragen behandelt, die die Hersteller dabei unterstützen, zu klären, ob ihr Produkt mit digitalen Elementen Datenfernverarbeitungslösungen enthält (siehe Abschnitt *8.1 Was gilt als Datenfernverarbeitungslösung für ein Produkt mit digitalen Elementen?*). Anschließend wird auf die technischen Auswirkungen von Datenfernverarbeitungslösungen und auf die Frage eingegangen, wie die Einhaltung der Cyberresilienzverordnung zu bewerten ist (siehe Abschnitt *8.2 Praktische und technische Auswirkungen von Datenfernverarbeitungslösungen und Rückgriff auf Lösungen Dritter*).

180. In Artikel 3 Nummer 2 ist der Begriff „Datenfernverarbeitung“ definiert als „entfernt stattfindende Datenverarbeitung, für die eine Software vom Hersteller selbst oder unter dessen Verantwortung konzipiert und entwickelt wird und ohne die das Produkt mit digitalen Elementen eine seiner Funktionen nicht erfüllen könnte“. Datenfernverarbeitungslösungen sind folglich definiert als die Softwareelemente (der „Teil eines elektronischen Informationssystems, der aus Computercode besteht“, wie in Artikel 3 Nummer 4 definiert) der Datenverarbeitung aus der Ferne. Als Teil des Gesamtpakets des Produkts mit digitalen Elementen sollen sie nicht die Hardware enthalten, auf deren Grundlage die Datenfernverarbeitung möglicherweise erfolgt.

181. In den Erwägungsgründen 11 und 12 wird näher erläutert, wie dieser Begriff ausgelegt werden sollte. In Erwägungsgrund 11 wird klargestellt, dass das Ziel der Einbeziehung von Datenfernverarbeitungslösungen darin besteht, dass die „Produkte in ihrer Gesamtheit von ihren Herstellern angemessen gesichert werden, unabhängig davon, ob die Daten lokal auf dem Gerät des Nutzers oder aus der Ferne durch den Hersteller verarbeitet oder gespeichert werden“. Außerdem heißt es dort: „Die Anforderungen an Datenfernverarbeitungslösungen, die in den Anwendungsbereich dieser Verordnung fallen, beinhalten daher keine technischen, betrieblichen oder organisatorischen Maßnahmen zur Beherrschung der Risiken für die Sicherheit der Netz- und Informationssysteme des Herstellers insgesamt.“

182. Folglich geht aus Erwägungsgrund 11 hervor, dass die Anforderungen der Cyberresilienzverordnung nicht die gesamte IT-Infrastruktur einer Organisation abdecken sollen, sondern nur Softwarekomponenten, die die Ausführung der Datenverarbeitungslösung ermöglichen. Beispielsweise sollten interne Systeme, die sich auf die eigenen Humanressourcen des Herstellers, Gehaltslisten, Kundenbeziehungsmanagement, Pipelines für die kontinuierliche Integration/kontinuierliche Lieferung (CI/CD) und die Verteilung von Sicherheitsaktualisierungen an Edge-Standorten beziehen, nicht als Datenfernverarbeitungslösungen betrachtet werden. Ebenso fallen Systeme im Zusammenhang mit Audit- und Testtätigkeiten wie Penetrationstests, Bedrohungsjagd und Red-Teaming nicht unter Produkte mit digitalen Elementen im Anwendungsbereich der Cyberresilienzverordnung. Es sei darauf hingewiesen, dass die Durchführung wirksamer und regelmäßiger Tests und Überprüfungen der Sicherheit des Produkts mit digitalen Elementen zwar eine wesentliche Anforderung gemäß Anhang I Teil II Nummer 3 der Cyberresilienzverordnung ist, dies jedoch nicht bedeutet, dass solche Tätigkeiten als Datenfernverarbeitungslösungen für das Produkt mit digitalen Elementen zu betrachten sind.

183. Schwerpunkt von Erwägungsgrund 12 sind Cloud-Dienste; dabei wird auch auf die Umstände eingegangen, unter denen Cloud-Dienste als Datenfernverarbeitungslösungen betrachtet werden könnten. Abschließend wird in dem Erwägungsgrund darauf hingewiesen, dass Cloud-Computing-Dienste und Cloud-Dienstmodelle in den Anwendungsbereich der Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie) ([28]) fallen, in der Anforderungen an das Risikomanagement im Bereich der Cybersicherheit für Anbieter von Cloud-Computing-Diensten festgelegt sind. Diese Anforderungen werden in der Durchführungsverordnung (EU) 2024/2690 ([29]) der Kommission näher ausgeführt.

8.1. **Was gilt als Datenfernverarbeitungslösung für ein Produkt mit digitalen Elementen?**

184. Die Definition des Begriffs „Datenfernverarbeitung“ in Artikel 3 Nummer 2 stützt sich somit auf drei Elemente: i) ob die Datenverarbeitung „entfernt stattfindet“; ii) ob das Produkt mit digitalen Elementen ohne eine solche Datenverarbeitung eine seiner Funktionen nicht erfüllen könnte und iii) ob die Software vom Hersteller oder unter seiner Verantwortung konzipiert und entwickelt wird. In den folgenden drei Unterabschnitten wird auf jedes dieser Elemente näher eingegangen.

([28]) Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27).

([29]) Durchführungsverordnung (EU) 2024/2690 der Kommission vom 17. Oktober 2024 mit Durchführungsbestimmungen zur Richtlinie (EU) 2022/2555 im Hinblick auf die technischen und methodischen Anforderungen der Risikomanagementmaßnahmen im Bereich der Cybersicherheit und die Präzisierung der Fälle, in denen ein Sicherheitsvorfall in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter als erheblich gilt (ABl. L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

8.1.1. *Der Begriff „entfernt stattfindend“*

185. Der in Artikel 3 Nummer 2 verwendete Begriff „entfernt stattfindend“ ist relevant, reicht aber nicht aus, um festzustellen, ob ein Produkt mit digitalen Elementen Datenfernverarbeitungslösungen umfasst. Darüber hinaus ist es angesichts der Vielfalt der Lösungen, die unter diesen Begriff fallen könnten, nicht möglich, den Begriff „entfernt stattfindend“ erschöpfend zu definieren. Folglich ist eine Einzelfallbewertung durch den Hersteller erforderlich.

186. Im Erwägungsgrund 11 der Cyberresilienzverordnung werden Daten erwähnt, die „aus der Ferne durch den Hersteller“ verarbeitet oder gespeichert werden, im Gegensatz zu Daten, die „lokal auf dem Gerät des Nutzers“ verarbeitet oder gespeichert werden. Datenfernverarbeitung erfolgt in der Regel außerhalb der Nutzerumgebung eines Produkts mit digitalen Elementen oder der Betriebsumgebung einer Organisation (für einen beruflichen Nutzer). Dies schließt jedoch nicht aus, dass die Verarbeitung auch in der Nähe des Geräts („dezentral“) erfolgt. Die Datenübertragung kann drahtgebunden (beispielsweise über ein Ethernetkabel) oder drahtlos (beispielsweise über WLAN oder Bluetooth) erfolgen. Cloud-Computing, einschließlich Edge Computing, ist ein typisches Beispiel für die „entfernte“ Datenverarbeitung. Beispielsweise erfolgt im Falle einer cloudgestützten Funktion, auf die der Nutzer über eine mobile Anwendung zugreift, ein Teil der Datenverarbeitung in der Cloud außerhalb der Umgebung des Nutzers.

187. Es sei darauf hingewiesen, dass Datenfernverarbeitungslösungen nicht unbedingt auf Cloud-Infrastrukturen Dritter betrieben werden. Die auf lokalen Servern in den Räumlichkeiten des Herstellers durchgeführte Datenfernverarbeitung kann ebenfalls eine Datenfernverarbeitungslösung darstellen. Mit anderen Worten, eine Lösung, die vor Ort und in einer privaten Cloud betrieben wird, kann gleichermaßen als Datenfernverarbeitungslösung eingestuft werden wie eine Lösung, die in einer öffentlichen Cloud und entfernten Räumlichkeiten betrieben wird.

188. Die beiden entscheidenden und kumulativen Fragen, über die sich bestimmt, ob die Datenverarbeitung als Datenfernverarbeitungslösung in den Anwendungsbereich der Cyberresilienzverordnung fällt, sind nachstehend in den Abschnitten *8.1.2* und *8.2* dargelegt. Wenn beide Fragen bejaht werden, gilt die Datenfernverarbeitung als Datenfernverarbeitungslösung.

8.1.2. *Würde das Produkt mit digitalen Elementen ohne eine solche Datenverarbeitung eine seiner Funktionen nicht erfüllen können?*

189. Wie in der Definition des Begriffs „Datenfernverarbeitung“ in Artikel 3 Nummer 2 festgelegt, sind die Voraussetzungen für Datenfernverarbeitung dann erfüllt, wenn das Produkt mit digitalen Elementen ohne diese Verarbeitung eine seiner Funktionen nicht erfüllen könnte. Der in dieser Definition enthaltene Begriff „Funktionen“ ist nicht auf die „Kernfunktionen“ oder die „Zweckbestimmung“ des Produkts mit digitalen Elementen beschränkt, da die Cyberresilienzverordnung keine solche Beschränkung vorsieht. Bei den Funktionen, die in den Anwendungsbereich der Cyberresilienzverordnung fallen, handelt es sich sowohl um Funktionen, die die von den Nutzern wahrgenommene Zweckbestimmung des Produkts mit digitalen Elementen unmittelbar erfüllen, als auch um Funktionen, die die Gesamtleistung des Produkts unterstützen.

190. Als Beispiele für Funktionen, bei denen eine Datenverarbeitung aus der Ferne stattfinden kann und deren Fehlen dazu führen würde, dass ein Produkt mit digitalen Elementen eine seiner Funktionen nicht mehr erfüllen könnte, sind zu nennen: i) Senden von Befehlen an ein Gerät; ii) Synchronisierung von Dateien; iii) Onboarding eines Nutzers; iv) Konfiguration (Personalisierung des Produkts mit digitalen Elementen); v) automatisierte Verbreitung von Aktualisierungen, einschließlich Funktionsaktualisierung und Sicherheits-Patches; vi) Identitäts- und Zugangsmanagement.

191. In einigen Fällen kann der Nutzer eine Funktion sowohl aus der Ferne als auch manuell nutzen (beispielsweise das Schalten einer Glühlampe mit einer App oder manuell). Diese Option schließt nicht aus, dass die Datenverarbeitung im Zusammenhang mit der entfernten Ausführung der Funktion als Datenfernverarbeitungslösung eingestuft wird. Die entfernte Ausführung dieser Funktion wird auch als Teil der Funktionen betrachtet, die das Produkt mit digitalen Elementen bietet.

192. Wenn hingegen das Produkt mit digitalen Elementen durch das Fehlen einer bestimmten Datenverarbeitung nicht daran gehindert ist, eine seiner Funktionen zu erfüllen, gilt eine solche Verarbeitung nicht als Datenfernverarbeitungslösung im Sinne der Cyberresilienzverordnung. Dazu gehört auch beispielsweise die Fernanalyse von Telemetriedaten, die ausschließlich für statistische Zwecke oder die künftige Produktentwicklung erhoben werden.

193. Doch selbst wenn die Datenverarbeitung eine Funktion eines Produkts mit digitalen Elementen nicht unterstützt, müssen die Hersteller im Rahmen ihrer Bewertung der Cybersicherheitsrisiken möglicherweise überlegen, ob mit diesen Fernkomponenten Risiken für das Produkt mit digitalen Elementen verbunden sind (beispielsweise angesichts der Betriebsumgebung des Produkts), und diese Risiken entsprechend mindern (beispielsweise durch Risikominderung auf Produktebene).

194. Websites sind ein Sonderfall, der einer weiteren Klärung bedarf, wie auch in Abschnitt *2.1 Inverkehrbringen* erläutert wird. Websites fallen nicht in den Anwendungsbereich von Datenfernverarbeitungslösungen, sofern sie nicht eine Funktion eines Produkts mit digitalen Elementen unterstützen, wie in Erwägungsgrund 11 der Cyberresilienzverordnung erläutert. Allein die Tatsache, dass eine Website Informationen über ein Produkt mit digitalen Elementen enthält, reicht nicht dafür aus, dass diese Website in den Anwendungsbereich von Datenfernverarbeitungslösungen fällt, selbst wenn von dem Produkt eine Weiterleitung zu einer solchen Website erfolgt. So ist beispielsweise die Weiterleitung von Nutzern zu einer externen Website mit Informationen und Anweisungen für die Nutzer keine Datenfernverarbeitungslösung. Dagegen kann eine Website in den Anwendungsbereich von Datenfernverarbeitungslösungen fallen, wenn sie eine Funktion eines Produkts mit digitalen Elementen ermöglicht oder unterstützt. Beispielsweise würde ein Authentifizierungsportal, das Berechtigungsnachweise oder Tokens ausstellt, die für den Betrieb des Produkts mit digitalen Elementen erforderlich sind, als Datenfernverarbeitungslösung gelten (sofern auch die anderen Kriterien der Definition erfüllt sind).

8.1.3. *Wurde die Software vom Hersteller oder unter dessen Verantwortung konzipiert und entwickelt?*

195. In der Definition des Begriffs „Datenfernverarbeitung“ in Artikel 3 Nummer 2 der Cyberresilienzverordnung ist ferner festgelegt, dass die Software für eine solche Datenfernverarbeitung vom Hersteller selbst oder unter dessen Verantwortung konzipiert und entwickelt werden muss. Eine Datenfernverarbeitung, die vollständig vom Hersteller (intern) entwickelt und konzipiert wurde, würde natürlich als Datenfernverarbeitungslösung gelten. Dies wäre auch der Fall, wenn Hersteller die Entwicklung und Konzeption einer Lösung einem externen Dienstleister überlassen (d. h., diese Arbeit „unter ihrer Verantwortung“ erfolgt). Die Formulierung „unter dessen [des Herstellers] Verantwortung“ bezieht sich auf Fernverarbeitungslösungen, die speziell auf den Hersteller zugeschnitten sind. Hierbei handelt es sich um Fälle, in denen der Hersteller nicht nur ein bestehendes Produkt mit digitalen Elementen oder eine bestehende Dienstleistung, die ein Diensteanbieter seinen Kunden anbietet, oder leicht abgewandelte Versionen davon lizenziert. „Unter dessen [des Herstellers] Verantwortung“ bedeutet, dass die Software ausschließlich vom Hersteller oder in seinem Namen auf Grundlage der von ihm bereitgestellten Entwürfe und Spezifikationen erstellt wird.

196. Für die Auslegung des Begriffs „Datenfernverarbeitungslösung“ ist die Tatsache, „wer die Lösung betreibt“ kein entscheidender Faktor, da sich die in der Cyberresilienzverordnung enthaltene Definition nur auf die Konzeption und Entwicklung der Datenfernverarbeitungslösung bezieht. Dies steht im Einklang mit dem in der Cyberresilienzverordnung verfolgten Ansatz, wonach die Anforderungen und Pflichten auf der Seite der Hersteller und nicht auf der Seite des Betriebs des Produkts mit digitalen Elementen liegen. Wenn Hersteller Lösungen konzipieren und entwickeln, die dann von einem Dritten betrieben werden, bleiben sie für die Einhaltung der grundlegenden Anforderungen der Cyberresilienzverordnung an das von ihnen in den Verkehr gebrachte Produkt mit digitalen Elementen verantwortlich.

197. Es muss unterschieden werden zwischen Fällen, in denen die Konzeption und Entwicklung von den Herstellern (oder unter ihrer Verantwortung) durchgeführt wird, und Fällen, in denen auf Lösungen Dritter zurückgegriffen wird, die nicht von Herstellern (oder unter ihrer Verantwortung) konzipiert und entwickelt wurden. Beispielsweise ist es hilfreich, die gängigsten Cloud-Dienstmodelle zu berücksichtigen, die unterschiedliche Grade der Nutzerkontrolle bieten und auch in Erwägungsgrund 12 der Cyberresilienzverordnung genannt sind, nämlich Software als Dienstleistung (*Software-as-a-Service*, SaaS), Plattform als Dienstleistung (*Platform-as-a-Service*, PaaS) und Infrastruktur als Dienstleistung (*Infrastructure-as-a-Service*, IaaS).

198. Im Falle einer IaaS-Lösung eines Dritten verwaltet oder kontrolliert der Hersteller die zugrunde liegenden physischen und virtuellen Ressourcen (wie die zugrunde liegende Hardware und den Hypervisor des Cloud-Diensteanbieters) nicht, sondern ist in der Lage, beliebige Software unter Verwendung dieser Ressourcen, wie Betriebssysteme und Anwendungen, zu installieren und zu betreiben. Eine solche Software wird vom Hersteller oder unter seiner Verantwortung konzipiert und entwickelt und kann daher als Datenfernverarbeitungslösungen eingestuft werden (sofern sie die anderen Elemente der Definition erfüllt).

199. Im Falle einer PaaS-Lösung eines Dritten setzt der Hersteller seine eigene (erstellte oder erworbene) Anwendung unter Verwendung der vom Cloud-Dienstleister bereitgestellten Programmiersprachen und Ausführungsumgebungen ein und integriert die Anwendung in sein Produkt mit digitalen Elementen. Der Hersteller hat die Kontrolle über die Anwendung und möglicherweise über die Konfigurationseinstellungen für die Ausführungsumgebung. Die Anwendung wird daher vom Hersteller oder unter seiner Verantwortung konzipiert und entwickelt und kann daher als Datenfernverarbeitungslösung eingestuft werden (sofern sie die anderen Elemente der Definition erfüllt).

200. Im Falle einer SaaS-Lösung eines Dritten bietet der SaaS-Anbieter dem Hersteller eine vollständig entwickelte Anwendung an, die in das Produkt des Herstellers mit digitalen Elementen integriert werden soll. Der Hersteller ist nur begrenzt in der Lage, nutzerspezifische Anwendungskonfigurationseinstellungen zu verwalten. Die Anwendung wird daher weder vom Hersteller selbst noch unter seiner Verantwortung konzipiert und entwickelt.

201. Wenn jedoch bestimmte Elemente nicht als Datenfernverarbeitungslösungen gelten (beispielsweise der Hypervisor im Falle einer IaaS-Infrastruktur eines Dritten, das Betriebssystem im Falle einer PaaS-Lösung eines Dritten oder die SaaS-Anwendung eines Dritten), sondern in einer Weise in das Produkt mit digitalen Elementen integriert sind, die sich auf dessen Sicherheit auswirkt, sollten solche Lösungen als mit Komponenten Dritter vergleichbar angesehen werden. Der Hersteller ist verpflichtet, Risiken im Zusammenhang mit der Integration dieser Elemente zu ermitteln und zu bewerten und ihnen zu begegnen, indem er die grundlegenden Anforderungen an das Produkt mit digitalen Elementen selbst umsetzt. Dies kann gegebenenfalls durch die Sicherheitsfunktionen unterstützt werden, die der Cloud-Dienstleister im Rahmen seines Modells der geteilten Verantwortung bereitstellt, wenn der Hersteller diese Funktionen nutzt oder konfiguriert, um den ermittelten Risiken zu begegnen. Darüber hinaus wird vom Hersteller erwartet, dass er eine ähnliche Verpflichtung wie die in Artikel 13 Absatz 5 genannte Pflicht zur Erfüllung der Sorgfaltspflicht in Bezug auf die Sicherheit dieser Komponenten in einer Weise erfüllt, die in einem angemessenen Verhältnis zu dem Risiko steht, das die Fernlösung für die Sicherheit des Produkts mit digitalen Elementen darstellt.

202. Daher lässt sich Folgendes zusammenfassen:

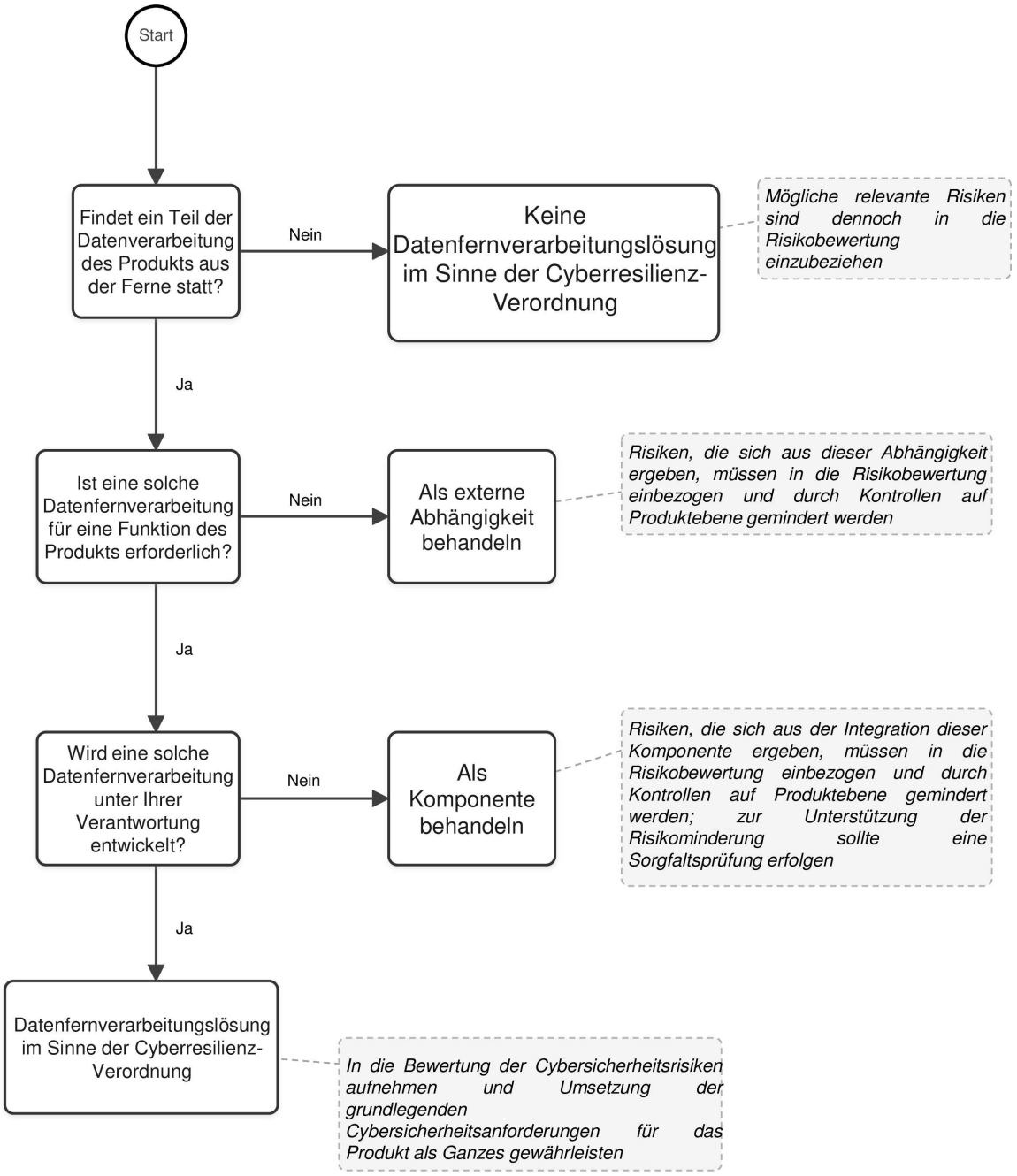
a) Damit Datenverarbeitung als Datenfernverarbeitungslösung eingestuft wird, müssen die beiden in den Abschnitten *8.1.2 Würde das Produkt mit digitalen Elementen ohne eine solche Datenverarbeitung eine seiner Funktionen nicht erfüllen können?* und *8.1.3 Wurde die Software vom Hersteller oder unter dessen Verantwortung konzipiert und entwickelt?* gestellten Fragen bejaht werden.

b) Falls die in Abschnitt *8.1.2 Würde das Produkt mit digitalen Elementen ohne eine solche Datenverarbeitung eine seiner Funktionen nicht erfüllen können?* gestellte Frage verneint wird, sollten die Hersteller die Risiken, die sich aus einer solchen Datenverarbeitung ergeben, im Rahmen ihrer Risikobewertung bewerten.

c) Falls die in Abschnitt *8.1.2 Würde das Produkt mit digitalen Elementen ohne eine solche Datenverarbeitung eine seiner Funktionen nicht erfüllen können?* gestellte Frage bejaht wird, die in Abschnitt *8.1.3 Wurde die Software vom Hersteller oder unter dessen Verantwortung konzipiert und entwickelt?* gestellte Frage hingegen verneint wird, sollten die Hersteller die Lösung Dritter als Komponente behandeln. Im Rahmen der Risikobewertung sollten die Hersteller die Risiken, die sich aus der Integration einer solchen Lösung ergeben, bewerten und entsprechend mindern. Darüber hinaus sollten die Hersteller die gebotene Sorgfalt walten lassen.

Abbildung 9

Stilisiertes Flussdiagramm zur Feststellung, ob ein Produkt mit digitalen Elementen Datenfernverarbeitungslösungen enthält



8.2. Praktische und technische Auswirkungen von Datenfernverarbeitungslösungen und Rückgriff auf Lösungen Dritter

203. Die Cyberresilienzverordnung folgt einem risikobasierten Ansatz, der in Artikel 13 Absätze 2 und 3 sowie in der ersten grundlegenden Anforderung in Anhang I Teil I verankert ist, wonach „Produkte mit digitalen Elementen … so konzipiert, entwickelt und hergestellt [werden], dass sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten“. Folglich sollte bei der Anwendung der Anforderungen der Cyberresilienzverordnung auf Datenfernverarbeitungslösungen und bei der Behandlung von Risiken, die sich aus in das Produkt mit digitalen Elementen integrierten Dienstleistungen Dritter ergeben, ein risikobasierter Ansatz in Betracht gezogen werden.

204. Erstens sollten die Hersteller i) in der technischen Dokumentation angeben, dass ihr Produkt mit digitalen Elementen über Datenfernverarbeitungslösungen verfügt oder sich auf Fernlösungen Dritter stützt, und ii) solche Lösungen beschreiben. Wenn eine Datenfernverarbeitungslösung mehrere Produkte mit digitalen Elementen unterstützt, muss diese Datenfernverarbeitungslösung in der technischen Dokumentation jedes Produkts angegeben werden. Die Dokumentation zu einer Datenfernverarbeitungslösung, die durch mehrere Produkte mit digitalen Elementen nutzbar ist, kann von einer Produktkonformitätsbewertung zur nächsten wiederverwendet werden.

205. Wie in Erwägungsgrund 11 dargelegt, sollten Datenfernverarbeitungslösungen, die Teil des Produkts mit digitalen Elementen sind und daher der Konformitätsbewertung des Produkts unterliegen, auf diejenigen Softwaremodule beschränkt werden, die für die Funktionalität des Produkts mit digitalen Elementen verantwortlich sind, sowie auf die Schnittstellen, die diese Module mit externen Diensten nutzen. Weitere Back-End-Systeme, die eine anschließende Verarbeitung durchführen und mit denen das Produkt mit digitalen Elementen nicht direkt interagiert, gelten nicht als Datenfernverarbeitungslösungen.

206. Dennoch bleiben diese Back-End-Systeme externe Abhängigkeiten, die im Rahmen der Bewertung der Cybersicherheitsrisiken bewertet und durch Maßnahmen auf Produktebene gemindert werden müssen. Bei der vom Hersteller durchgeführten Risikobewertung sollte Folgendes berücksichtigt werden: i) Risiken im Zusammenhang mit Datenfernverarbeitungslösungen; ii) Risiken im Zusammenhang mit der Abhängigkeit von Fernlösungen Dritter (ähnlich Komponenten Dritter) und iii) Risiken im Zusammenhang mit der Produktumgebung (beispielsweise der zugrunde liegenden Hardware). Um diese Risiken zu mindern, sollten die Hersteller Sicherheitskontrollen am Produkt mit digitalen Elementen selbst durchführen.

207. Darüber hinaus kann im Rahmen der Konformitätsbewertung und/oder der Erfüllung der Sorgfaltspflichten im Zusammenhang mit Ferndiensten Dritter die folgende nicht erschöpfende Liste von Konformitätsnachweisen zur Unterstützung der Bewertung des Herstellers wiederverwendet werden:

a) Nachweis der Erfüllung der Verpflichtungen gemäß der Durchführungsverordnung (EU) 2024/2690 der Kommission,

b) Nachweis der Erfüllung der Verpflichtungen gemäß der Verordnung (EU) 2022/2554 (DORA),

c) Konformitätserklärung oder Zertifikat, das im Rahmen eines europäischen Systems für die Cybersicherheitszertifizierung (angenommen gemäß der Verordnung (EU) 2019/881, der Cybersicherheitsverordnung ausgestellt wurde,

d) Nachweis der Konformität mit ISO/IEC 27017:2015 oder ISO/IEC 27001:2022.

208. Schließlich müssen die Hersteller bei ihren Interaktionen mit Anbietern von Ferndiensten Dritter die am besten geeigneten Sicherheitsmaßnahmen auf der Grundlage ihrer Risikobewertung umsetzen (und werden dabei gegebenenfalls durch das Modell der geteilten Verantwortung des Anbieters unterstützt). Diese Risikominderungsmaßnahmen sollten Sicherheitskontrollen für ihre Produkte mit digitalen Elementen und die Überprüfung der von den Drittanbietern selbst bereitgestellten Sicherheitsmaßnahmen (Sorgfaltspflicht) umfassen. Ein Instrument zur Minderung solcher Risiken kann darin bestehen, Sicherheitsgarantien in ihre Dienstgütevereinbarungen (*Service Level Agreements*, SLAs) mit Drittanbietern aufzunehmen, einschließlich der Zusicherung, dass die Anbieter Schwachstellen angemessen behandeln. Eine wesentliche Änderung der von den Drittanbietern von Ferndiensten bereitgestellten Lösungen sollte nicht als wesentliche Änderung des Produkts mit digitalen Elementen gelten, da diese Elemente nicht in die Verantwortung des Herstellers fallen. Im Rahmen ihrer Sorgfaltspflichten und zur ordnungsgemäßen Minderung der Risiken, die sich aus der Inanspruchnahme von Drittanbietern ergeben, sind die Hersteller jedoch aufgefordert, dafür zu sorgen, dass ihre externen Cloud-Dienstleister sie angemessen über Änderungen informieren, die sie an ihren Lösungen vornehmen. Auf Grundlage dieser Informationen müssen die Hersteller ihre Risikobewertung möglicherweise überarbeiten. Bei der aktualisierten Risikobewertung sollte berücksichtigt werden, ob die externen Diensteanbieter nach wie vor ausreichende Garantien in Bezug auf die Cybersicherheit bieten und ob die Sicherheitskontrollen auf Produktebene nach wie vor angemessen sind. In einigen Fällen müssen die Hersteller diese Kontrollen möglicherweise ändern oder externe Diensteanbieter wechseln.

8.3. **Anwendungsfälle für Datenfernverarbeitungslösungen**

Um den Herstellern zusätzliche praktische Orientierungshilfe zu geben, wird in diesem Abschnitt auf eine Reihe fiktiver Anwendungsfälle eingegangen, in denen archetypische Produkte mit digitalen Elementen beschrieben sind, die auf Datenfernverarbeitung beruhen, und veranschaulicht wird, ob eine solche Verarbeitung als Datenfernverarbeitungslösung im Sinne der Cyberresilienzverordnung einzustufen ist.

8.3.1. *Mobile Bankanwendung*

Ein Finanzunternehmen bringt eine mobile Bankanwendung in den Verkehr. Die Back-End-Systeme der App unterstützen unter anderem Authentifizierung, Autorisierung, Kontoverwaltung und Zahlungen. Zur Unterstützung der Funktionen der App nutzt das Finanzunternehmen eine hybride Strategie, die sich auf interne Infrastruktur sowie Fernlösungen Dritter stützt. Dazu zählen:

Selbst gehostete Infrastruktur, die vom Finanzunternehmen entwickelt wurde:

— Der Kunde öffnet die mobile Bankanwendung und wird über die Bankenschnittstelle, eine selbst gehostete Lösung, die von dem Finanzunternehmen entwickelt wurde, die über die App übermittelten Anfragen erhält und die entsprechenden Antworten zurücksendet, authentifiziert. Die Bankenschnittstelle überprüft die Identität des Kunden durch Abfrage des Kontoverwaltungssystems und gewährt Zugang zur Anwendung.

— Der Kunde löst über die App eine Überweisung aus. Die App übermittelt die Anweisung an die Bankenschnittstelle, die eine entsprechende Anfrage an das Hauptbuchsystem übermittelt.

— Das Kontoverwaltungssystem und das Hauptbuchsystem, die beide von der Bank selbst gehostet werden, aber logisch von der Bankenschnittstelle getrennt sind, erfassen die Transaktion.

— Das Hauptbuchsystem sendet den Transaktionsstatus zurück an die Bankenschnittstelle, die dem Kunden das Ergebnis präsentiert.

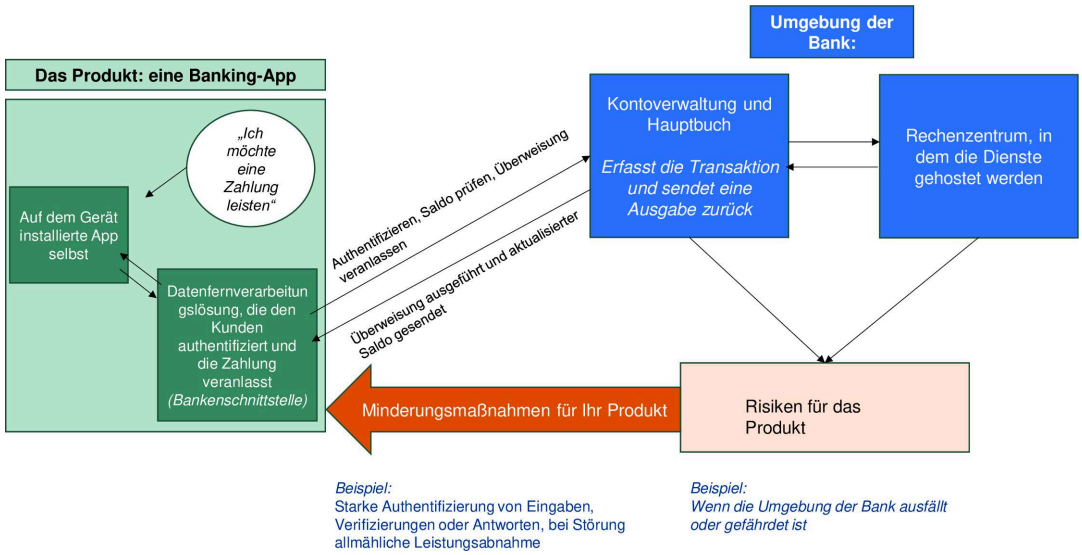
Auswirkungen auf Datenfernverarbeitungslösungen:

— Die Bankenschnittstelle ist erforderlich, damit die App ihre Funktionen erfüllen kann, nämlich die Authentifizierung des Kunden, die Übermittlung der Anweisungen des Kunden, einschließlich Zahlungs- und Überweisungsanweisungen, und die Rückgabe des sich daraus ergebenden Status. Die Bankenschnittstelle wird unter der Verantwortung des Herstellers konzipiert und entwickelt. Da die beiden in den vorhergehenden Abschnitten gestellten Fragen zu bejahen sind, ist die Bankenschnittstelle als Datenfernverarbeitungslösung zu betrachten. Sie muss daher in die Bewertung der Cybersicherheitsrisiken und in die Umsetzung der grundlegenden Anforderungen an das Produkt mit digitalen Elementen als Ganzes einbezogen werden. Die anschließende Verarbeitung einer einmal übermittelten Anweisung, insbesondere die Erfassung der Transaktion in den Kontoführungs- und Hauptbuchsystemen, die Abwicklung und das Clearing, erfolgt durch Systeme, mit denen die App nicht direkt interagiert, und stellt daher keine Datenfernverarbeitungslösung dar.

— Das Kontoführungssystem und das Hauptbuchsystem gelten für die Bankenanwendung nicht als Datenfernverarbeitungslösungen. Die App interagiert nicht direkt mit ihnen (sondern mit der Bankenschnittstelle, die wiederum von ihr abhängt). Obwohl ihre Verfügbarkeit für die Ausführung einer Funktion erforderlich sein kann, deckt die Cyberresilienzverordnung nur jene Teile des Systems ab, die direkt mit dem Produkt mit digitalen Elementen interagieren. Sie fallen daher für die Zwecke der Cyberresilienzverordnung nicht unter die Definition „Datenfernverarbeitungslösungen“. Diese Systeme bleiben jedoch externe Abhängigkeiten, die zu erheblichen Cybersicherheitsrisiken für das Produkt mit digitalen Elementen führen können. Ein Angriff auf das Hauptbuchsystem könnte es beispielsweise dem Angreifer ermöglichen, Transaktionsergebnisse zu beeinflussen, die anschließend in der Anwendung angezeigt werden. Der Hersteller ist daher verpflichtet, diese Risiken im Rahmen der Bewertung der Cybersicherheitsrisiken zu ermitteln und zu bewerten und sie durch Maßnahmen auf Produktebene zu mindern, wie beispielsweise eine starke Authentifizierung von Back-End-Schnittstellen, den Schutz der Integrität von Transaktionsdaten, sichere Kommunikationskanäle und die Überprüfung der von der App erhaltenen Antworten.

Abbildung 10

Stilisierte Darstellung einer auf Datenfernverarbeitungslösungen gestützten Banken-App



SaaS Dritter zur Kundenbetreuung:

— Das Finanzunternehmen integriert in seine App eine Chat-Lösung für den Kunden-Support, die von einem Drittanbieter entwickelt und betrieben wird; der Drittanbieter hat den Code für den Chat-Server geschrieben, die Benutzerschnittstelle aufgebaut und betreibt die Infrastruktur, in der der Chat stattfindet (also ein SaaS-Modell).

— Wenn der Kunde eine Support-Anfrage stellt, verbindet die App den Kunden mit dem externen Dienst, über den die Chat-Sitzung aufgebaut und der Nachrichtenaustausch abgewickelt wird, ohne dem Dritten Zugang zu den Kernsystemen der Bank zu gewähren.

Auswirkungen auf Datenfernverarbeitungslösungen:

— Die Support-Chat-Lösung ist erforderlich, damit das Produkt mit digitalen Elementen eine seiner Funktionen erfüllen kann, wird jedoch weder vom Finanzunternehmen noch unter seiner Verantwortung konzipiert und entwickelt; es handelt sich daher nicht um eine Datenfernverarbeitungslösung. Die Lösung sollte jedoch wie eine Komponente eines Dritten behandelt werden. Die Abhängigkeit von diesem externen Dienst kann Cybersicherheitsrisiken für die Bankenanwendung mit sich bringen, beispielsweise wenn ein Angreifer den Chat-Kanal nutzen würde, um sich als Bank auszugeben oder an Nutzer böswillige Inhalte zu übermitteln. Das Finanzunternehmen muss diese Risiken bei seiner Bewertung der Cybersicherheitsrisiken berücksichtigen und diese Risiken durch Maßnahmen auf Produktebene mindern, wie beispielsweise die Trennung der Chat-Funktion von den Kernfunktionen der Bank, die Kontrolle der Datenströme und die Validierung von Inhalten. Die Sorgfaltspflicht in Bezug auf die SaaS sollte ebenfalls erfüllt werden.

8.3.2. *Intelligenter Thermostat*

Ein intelligenter Thermostat ermöglicht es den Nutzern, die Temperatur ihrer Wohnungen über eine mobile Anwendung zu steuern. Die mobile Anwendung und der intelligente Thermostat sind auf Datenfernverarbeitung angewiesen, um Daten auszutauschen (beispielsweise einen Befehl zur Temperaturerhöhung) und zu speichern (beispielsweise Nutzerpräferenzen). Diese Funktionen wurden unter der Verantwortung des Herstellers entwickelt und konzipiert, laufen jedoch auf einer zugrunde liegenden physischen und virtuellen Infrastruktur, die von einem Dritten (IaaS eines Dritten) bereitgestellt wird.

Da der intelligente Thermostat seine intelligenten Funktionen ohne diese Datenfernverarbeitung nicht ausführen könnte, würde ihr Fehlen das Produkt mit digitalen Elementen daran hindern, eine oder mehrere seiner Funktionen zu erfüllen. Darüber hinaus wurde die Software unter der Verantwortung des Herstellers des intelligenten Thermostats entwickelt und konzipiert. Daher gilt die Datenfernverarbeitung als Datenfernverarbeitungslösung im Sinne der Cyberresilienzverordnung.

Für die Zwecke der Einhaltung der Cyberresilienzverordnung muss der Hersteller des intelligenten Thermostats die Datenfernverarbeitungslösungen sowie die Abhängigkeit von der IaaS eines Dritten in der technischen Dokumentation des Produkts mit digitalen Elementen, einschließlich der Einzelheiten der vertraglich vereinbarten Dienstleistung, dokumentieren. Der Hersteller muss diese Elemente bei der Risikobewertung berücksichtigen, was auch für die Zweckbestimmung und die vernünftigerweise vorhersehbare Verwendung des Produkts mit digitalen Elementen gilt. Der Hersteller setzt die grundlegenden Anforderungen der Cyberresilienzverordnung auf Grundlage der Risiken der Datenfernverarbeitungslösungen um. In Bezug auf die IaaS eines Dritten muss der Hersteller sicherstellen, dass die vom Drittanbieter bereitgestellten Sicherheitsmaßnahmen angemessen sind, und/oder einschlägige Maßnahmen in Bezug auf die Infrastruktur ergreifen. Im erstgenannten Fall könnte der Hersteller beispielsweise Nachweise dafür verlangen, dass die NIS-2-Verpflichtungen erfüllt wurden.

8.3.3. *E-Reader*

Der Hersteller einer E-Reader-Software nutzt einen externen SaaS-Speicherdienst, um von Kunden gekaufte elektronische Bücher zu speichern und den Kunden den Zugang zu ihren Büchern zu ermöglichen. Bei einem Fehlen dieses Speicherdienstes könnte das Produkt mit digitalen Elementen eine seiner Funktionen nicht erfüllen, allerdings wurde der SaaS-Speicherdienst weder vom Hersteller selbst noch unter seiner Verantwortung entwickelt; der SaaS-Anbieter stellt ihn den Kunden für jeden Anwendungsfall zur Verfügung.

Der SaaS-Speicherdienst entspricht nicht der Definition von Datenfernverarbeitungslösungen. Der Hersteller des E-Readers stützt sich jedoch für das Funktionieren seines Produkts mit digitalen Elementen auf diesen externen Dienst und muss daher bei seiner Bewertung der Cybersicherheitsrisiken die damit verbundenen Risiken berücksichtigen. Der Hersteller des E-Readers sollte die SaaS wie eine Komponente behandeln. Der Hersteller muss auf Produktebene geeignete Sicherheitsmaßnahmen umsetzen, wie beispielsweise sichere Authentifizierung, Verschlüsselung und Schutz der Integrität der Kommunikation mit dem Speicherdienst. Die Wahrnehmung der Sorgfaltspflicht bei der Auswahl und Integration des SaaS-Anbieters wird auch die Erfüllung der Pflichten des Herstellers unterstützen, damit das Produkt mit digitalen Elementen als Ganzes die grundlegenden Anforderungen erfüllen kann.

8.3.4. *Industrieroboter*

Ein Industrieroboter hat die Aufgabe, Teile aufzunehmen. Der Roboter sendet die über Kameras erfassten Informationen an einen vom Hersteller konzipierten und entwickelten Ferndienst. Dieser Dienst läuft auf einer zugrunde liegenden physischen und virtuellen Infrastruktur, die von einem externen Dienstleister bereitgestellt wird (externe IaaS). Der Cloud-Dienst berechnet die Position eines Teils auf Grundlage der Kamera-Feeds und sendet Befehle zurück an den Roboter, damit dieser die Teile aufnimmt.

Ohne diese Datenverarbeitung wäre der Industrieroboter nicht in der Lage, Teile aufzunehmen, und könnte somit eine seiner Funktionen nicht erfüllen. Darüber hinaus wurde die auf der Infrastruktur laufende Software vom Hersteller konzipiert und entwickelt. Die vom Hersteller konzipierte und entwickelte Software entspricht der Definition von Datenfernverarbeitungslösungen.

Der Hersteller des Industrieroboters muss die Datenfernverarbeitungslösung sowie die Abhängigkeit von der IaaS eines Dritten in der technischen Dokumentation des Produkts mit digitalen Elementen (einschließlich Einzelheiten der vertraglich vereinbarten Dienstleistung) dokumentieren. Der Hersteller muss diese Elemente auch bei der Risikobewertung berücksichtigen, die die Zweckbestimmung und die vernünftigerweise vorhersehbare Verwendung des Produkts mit digitalen Elementen umfasst. Der Hersteller setzt die grundlegenden Anforderungen der Cyberresilienzverordnung an das Produkt mit digitalen Elementen, einschließlich seiner Datenfernverarbeitungslösung, auf der Grundlage der Risiken um. Die Sorgfaltspflicht bei der Auswahl des IaaS-Anbieters wird auch die Erfüllung der Pflichten des Herstellers unterstützen. Beispielsweise könnte der Hersteller Nachweise dafür verlangen, dass NIS-2-Verpflichtungen erfüllt wurden.

8.3.5. *Mobilfunknetz*

Ein Smartphone stützt sich auf ein 5G-Netz, um seinen Nutzern Internetanschlüsse, Telefonanrufe und Nachrichten bereitzustellen (mobile Konnektivität). Das Mobilfunknetz wird von Telekommunikationsunternehmen entwickelt und konzipiert. Das Netz umfasst kleine Zellen und Zelltürme sowie weitere Netzausrüstung.

Das Produkt mit digitalen Elementen sollte in der Lage sein, sich ordnungsgemäß mit einem Netz zu verbinden; dies ist eine seiner Aufgaben. Ob dieses Netz in Betrieb ist oder nicht, ist jedoch für die Feststellung, ob das Produkt mit digitalen Elementen ordnungsgemäß funktioniert, nicht relevant. Das Netz ist nur ein Kommunikationskanal und nicht erforderlich, damit das Produkt mit digitalen Elementen seine Funktion der „ordnungsgemäßen Verbindung mit einem Netz" erfüllen kann. Ebenso gilt ein Ethernetkabel, ein Router oder ein WLAN-Signal nicht als Datenverarbeitung, ohne die das Produkt mit digitalen Elementen eine seiner Funktionen nicht erfüllen könnte, sondern vielmehr als Element, das Kommunikation/Konnektivität ermöglicht.

Folglich entspricht das Mobilfunknetz nicht der Definition von Datenfernverarbeitungslösungen. Das Netz sollte nicht wie eine Komponente eines Dritten betrachtet werden, da es keine in das Produkt mit digitalen Elementen integrierte Software gibt, sondern das Produkt sich lediglich auf dieses Netz stützt. Daher unterliegt der Hersteller keinen Sorgfaltspflichten gegenüber dem Netzbetreiber.

9. **WEITERE ELEMENTE**

9.1. **Meldepflichten**

209. Nach Artikel 14 Absätze 1 und 3 der Cyberresilienzverordnung ist der Hersteller verpflichtet, gleichzeitig dem als Koordinator benannten CSIRT und der ENISA i) jede aktiv ausgenutzte Schwachstelle, die in seinem Produkt mit digitalen Elementen enthalten ist und von der er Kenntnis erlangt, und ii) jeden schwerwiegenden Sicherheitsvorfall, der sich auf die Sicherheit des Produkts mit digitalen Elementen auswirkt und von dem er Kenntnis erlangt, zu melden.

210. Gemäß Artikel 69 Absatz 3 und Artikel 71 Absatz 2 Satz 2 gilt die Verpflichtung zur Einhaltung von Artikel 14 ab dem 11. September 2026 für alle Produkte mit digitalen Elementen, die in den Anwendungsbereich der Cyberresilienzverordnung fallen, einschließlich vor dem 11. Dezember 2027 in den Verkehr gebrachten Produkten mit digitalen Elementen. Im Gegensatz zu den Pflichten zur Behandlung von Schwachstellen, die nur für die Dauer des Unterstützungszeitraums eines Produkts gelten, gelten die Meldepflichten auch dann weiter, wenn ein Produkt mit digitalen Elementen nicht mehr unterstützt wird. Wurde ein Produkt mit digitalen Elementen vor dem 11. Dezember 2027 in den Verkehr gebracht oder ist der Unterstützungszeitraum abgelaufen, so ist der Hersteller nicht verpflichtet, die in Anhang I Teil II festgelegten Pflichten zur Behandlung von Schwachstellen zu erfüllen.

211. Es sei daran erinnert, dass die Verpflichtung zur Meldung solcher Ereignisse gilt, sobald der Hersteller Kenntnis davon erhält, dass eine Schwachstelle aktiv ausgenutzt wird oder dass ein schwerwiegender Sicherheitsvorfall aufgetreten ist, der zu einer Beeinträchtigung der Sicherheit seines Produkts mit digitalen Elementen geführt hat. Daher sollten Leitlinien dazu, wann davon ausgegangen wird, dass ein Hersteller Kenntnis erlangt hat, den Herstellern helfen, den Zeitpunkt zu bestimmen, zu dem die geltenden Meldefristen beginnen.

212. Hersteller können im Rahmen verschiedener EU-Rechtsakte vergleichbaren Meldepflichten unterliegen. Damit sichergestellt ist, dass der Begriff „Kenntnis erlangt" einheitlich ausgelegt wird, und um den Herstellern die Einhaltung der entsprechenden Pflichten zu erleichtern, stehen diese Leitlinien im Einklang mit Erwägungsgrund 31 der Durchführungsverordnung (EU) 2024/2690 der Kommission und Abschnitt II Buchstabe A der Leitlinien 9/2022 für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der DSGVO.

213. In einigen Fällen wird ein Hersteller ein verdächtiges Ereignis feststellen, oder ein Dritter, z. B. eine Person, ein Kunde, eine Einrichtung, eine Behörde, eine Medienorganisation oder eine andere Quelle, wird ihn auf einen potenziellen Sicherheitsvorfall oder eine potenzielle Schwachstelle aufmerksam machen. In solchen Fällen sollte der Hersteller das verdächtige Ereignis unverzüglich bewerten, um festzustellen, ob es sich um eine aktiv ausgenutzte Schwachstelle oder einen schwerwiegenden Sicherheitsvorfall mit Auswirkungen auf die Sicherheit des Produkts mit digitalen Elementen handelt. Es ist daher davon auszugehen, dass der Hersteller Kenntnis hatte, wenn er nach einer solchen Anfangsbewertung mit hinreichender Gewissheit feststellen kann, dass i) eine in seinem Produkt mit digitalen Elementen enthaltene Schwachstelle aktiv ausgenutzt wird oder ii) ein schwerwiegender Sicherheitsvorfall vorliegt, der zu einer Beeinträchtigung der Sicherheit seines Produkts mit digitalen Elementen geführt hat.

214. Daher hängt der Zeitpunkt, zu dem davon ausgegangen werden kann, dass ein Hersteller Kenntnis von der spezifischen aktiv ausgenutzten Schwachstelle oder dem schwerwiegenden Sicherheitsvorfall hat, von den Umständen ab. In einigen Fällen wird von Anfang an relativ klar sein, dass eine Schwachstelle aktiv ausgenutzt wird oder dass sich ein schwerwiegender Sicherheitsvorfall auf die Sicherheit eines Produkts mit digitalen Elementen auswirkt. In anderen Fällen kann es einige Zeit dauern, bis festgestellt ist, ob ein Produkt mit digitalen Elementen von einer Schwachstelle betroffen ist und ob diese Schwachstelle von einem böswilligen Akteur ausgenutzt wird oder ob sich ein Sicherheitsvorfall auf die Sicherheit eines Produkts mit digitalen Elementen auswirkt. Der Schwerpunkt sollte jedoch darauf liegen, dass rasche Maßnahmen zur Durchführung der Anfangsbewertung erfolgen, um festzustellen, ob diese Bedingungen tatsächlich erfüllt sind, insbesondere wenn die Schwachstelle ein erhebliches Risiko darstellen könnte, und wenn ja, um Abhilfemaßnahmen zu ergreifen und dies im Einklang mit der Cyberresilienzverordnung zu melden.

215. Darüber hinaus müssen die Hersteller aufgrund der Struktur der Meldepflichten ihre Meldungen schrittweise aktualisieren, wenn ihre internen Untersuchungen voranschreiten und sie mehr über die aktiv ausgenutzte Schwachstelle oder den Sicherheitsvorfall wissen. Insbesondere sind die Hersteller verpflichtet, unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Bekanntwerden, eine Frühwarnung mit begrenzten Informationen zu übermitteln. Im Anschluss daran sind zusätzliche Informationen im Rahmen der Meldung unverzüglich und in jedem Fall innerhalb von 72 Stunden nach Kenntnisnahme vorzulegen („72-Stunden-Meldung“). Der vollständige Bericht muss innerhalb von 14 Tagen, nachdem eine Korrektur- oder Risikominderungsmaßnahme für aktiv ausgenutzte Schwachstellen zur Verfügung steht, oder innerhalb eines Monats nach der 72-Stunden-Meldung schwerwiegender Sicherheitsvorfälle vorgelegt werden.

216. Wie in Abschnitt *3.3.1 Dauerhafte Unterstützung und Gewährleistung der Brauchbarkeit freier und quelloffener Software* dargelegt, sind Verwalter quelloffener Software auch verpflichtet, aktiv ausgenutzte Schwachstellen gemäß Artikel 24 Absatz 3 zu melden ([30]). Diese Verpflichtung gilt, sobald eine aktiv ausgenutzte Schwachstelle festgestellt wird, und nicht nur, wenn eine Schwachstelle in der Codebasis einer freien und quelloffenen Software besteht, für welche dieser Rechtsträger ein Verwalter ist. Da Komponenten freier und quelloffener Software in der Regel nachgelagert in andere Produkte mit digitalen Elementen integriert werden, wird ein Verwalter in der Praxis wahrscheinlich durch Berichte Dritter Kenntnis erlangen, die eine Ausnutzung in Komponenten freier und quelloffener Software, die in andere Produkte mit digitalen Elementen integriert ist, feststellen. Dies kann beispielsweise der Fall sein, wenn ein Hersteller eines Produkts mit digitalen Elementen die aktive Ausnutzung in einer in sein eigenes Produkt integrierten Komponente freier und quelloffener Software feststellt und dies dem Verwalter dieser Komponente meldet, oder wenn ein Nutzer oder ein Forscher im Bereich der Informationssicherheit Belege für die Ausnutzung einer in ein Produkt mit digitalen Elementen integrierten Komponente freier und quelloffener Software findet und diese aktive Ausnutzung dem Verwalter der Komponente meldet.

217. Es sollte auch klargestellt werden, dass der Hersteller nicht verpflichtet ist, Schwachstellen, deren aktive Ausnutzung ihm bereits vor dem 11. September 2026 (dem Datum, ab dem die Meldepflicht gilt) festgestellt hat, zu melden, da die Verpflichtung zur Meldung aktiv ausgenutzter Schwachstellen erst gilt, wenn er Kenntnis von der aktiven Ausnutzung erhält. Die Cyberresilienzverordnung schreibt daher keine rückwirkende Meldung solcher Schwachstellen vor. Dagegen gilt die Verpflichtung jedoch, wenn der Hersteller vor dem 11. September 2026 Kenntnis von einer Schwachstelle hatte, aber zu diesem Zeitpunkt keine Kenntnis von einer aktiven Ausnutzung dieser Schwachstelle hatte (entweder weil sie noch nicht aufgetreten war oder weil der Hersteller von ihr keine Kenntnis erlangt hatte). Erfolgt nach dem 11. September 2026 eine aktive Ausnutzung oder erlangt der Hersteller davon Kenntnis, gilt die Schwachstelle als aktiv ausgenutzt und unterliegt der Meldepflicht.

218. Ebenso ist ein Hersteller nur verpflichtet, aktiv ausgenutzte Schwachstellen in seinem Produkt mit digitalen Elementen zu melden. Enthält ein Produkt mit digitalen Elementen eine aktiv ausgenutzte Schwachstelle, deren Ursprung in einer Komponente eines Dritten liegt, so ist der Hersteller des Produkts mit digitalen Elementen verpflichtet, diese aktiv ausgenutzte Schwachstelle zu melden. Ist einem Hersteller jedoch bekannt, dass eine Komponente eines Dritten eine Schwachstelle enthält, diese Schwachstelle jedoch entweder i) in seinem Produkt mit digitalen Elementen nicht ausgenutzt werden kann (beispielsweise weil der anfällige Code nicht zugänglich ist) oder ii) in seinem Produkt mit digitalen Elementen nicht ausgenutzt wurde, so gilt diese Schwachstelle nicht als aktiv ausgenutzte Schwachstelle, die in seinem Produkt mit digitalen Elementen enthalten ist, und unterliegt daher für diesen Hersteller nicht der Meldepflicht. Dieser Hersteller kann diese Schwachstelle gemäß Artikel 15 der Cyberresilienzverordnung weiterhin auf freiwilliger Basis melden. Er ist ferner verpflichtet, die Anforderungen an die Behandlung von Schwachstellen gemäß Anhang I Teil II der Cyberresilienzverordnung zu erfüllen und die Schwachstelle der Person oder Einrichtung, die die Komponente herstellt oder wartet, gemäß Artikel 13 Absatz 6 und wie in Abschnitt *9.2.1 Vorgelagerte Meldung und gemeinsame Nutzung von Sicherheits-Patches* näher erläutert, zu melden.

([30]) Soweit der Verwalter an der Entwicklung eines Produkts mit digitalen Elementen beteiligt ist.

219. Nachdem Hersteller Kenntnis von einer aktiv ausgenutzten Schwachstelle oder einem schwerwiegenden Sicherheitsvorfall erhalten haben, sind sie gemäß Artikel 14 Absatz 8 auch verpflichtet, die betroffenen Nutzer und gegebenenfalls alle Nutzer zu informieren. Tun sie dies nicht rechtzeitig, können die CSIRTs, die die Meldung erhalten haben, den Nutzern diese Informationen zur Verfügung stellen, wenn dies als verhältnismäßig und erforderlich erachtet wird, um die Auswirkungen dieser Schwachstelle oder dieses Sicherheitsvorfalls zu verhindern oder zu mindern.

220. Im Einklang mit dem risikobasierten Ansatz der Cyberresilienzverordnung ist die in Artikel 14 Absatz 8 festgelegte Verpflichtung zur Information der Nutzer risikobasiert und verhältnismäßig anzuwenden. Insbesondere bedeutet die Weitergabe von Informationen über eine aktiv ausgenutzte Schwachstelle oder einen schwerwiegenden Sicherheitsvorfall nicht, dass diese Informationen unterschiedslos veröffentlicht oder offengelegt werden müssen. Gegebenenfalls können die Hersteller angesichts der Art des Produkts mit digitalen Elementen, der betroffenen Nutzer und der potenziellen Auswirkungen der Schwachstelle oder des Sicherheitsvorfalls die Offenlegung detaillierter Informationen auf die jeweils betroffenen Nutzer oder Kunden beschränken. Dies gilt insbesondere für Produkte mit digitalen Elementen, die in sensiblen oder wichtigen Umgebungen verwendet werden, in denen die Offenlegung technischer Einzelheiten an sich bereits die Cybersicherheitsrisiken erhöhen oder ihre weitere Ausnutzung erleichtern könnte.

221. Sobald die Schwachstelle angemessen behandelt oder gemindert wurde, kann eine umfassendere Offenlegung angemessen sein. Dies wäre beispielsweise der Fall, wenn die Offenlegung zur allgemeinen Sensibilisierung beiträgt oder es Nutzern ermöglicht, zu überprüfen, ob ihre Produkte mit digitalen Elementen nicht mehr betroffen sind. In solchen Fällen sollten die Detailtiefe und der Zeitpunkt einer umfassenderen Offenlegung verhältnismäßig bleiben und den Restrisiken einer Ausnutzung, der Art des Produkts mit digitalen Elementen und den Interessen der betroffenen Nutzer Rechnung tragen. Darüber hinaus sind die Hersteller gemäß Anhang I Teil II Nummer 4 verpflichtet, Informationen über behobene Schwachstellen offenzulegen, sobald eine Sicherheitsaktualisierung zur Verfügung gestellt wurde.

9.2. **Behandlung von Schwachstellen**

9.2.1. *Vorgelagerte Meldung und gemeinsame Nutzung von Sicherheits-Patches*

222. Nach Artikel 13 Absatz 6 der Cyberresilienzverordnung sind die Hersteller verpflichtet, Schwachstellen in integrierten Komponenten der Person oder Einrichtung zu melden, die diese Komponente herstellt oder wartet (im Folgenden „vorgelagerte Meldung“).

223. Hersteller sind nur in Bezug auf die bei ihnen integrierte Version der Komponente zu einer vorgelagerten Meldung verpflichtet. Wenn die Person oder Einrichtung, die die Komponente herstellt oder wartet, Sicherheitskonzepte, Verfahren zur koordinierten Offenlegung von Schwachstellen oder benannte Kanäle für die Meldung von Schwachstellen festgelegt hat, sollten die Hersteller im Einklang mit diesen Strategien ihre Meldung erstatten, insbesondere wenn eine vorzeitige Offenlegung von ungepatchten Schwachstellen die Cybersicherheitsrisiken erhöhen könnte. Um den Aufwand für vorgelagerte Wartungsbetriebe, insbesondere bei Open-Source-Projekten, zu verringern, sind die Hersteller zudem nicht verpflichtet, vorgelagerte Meldungen zu übermitteln, wenn sie bestätigen können, dass der Person oder Einrichtung, die eine Komponente herstellt oder wartet, die Schwachstelle bekannt ist. Die Hersteller sind aufgefordert, vor der Übermittlung einer vorgelagerten Meldung angemessene Maßnahmen zu ergreifen, um die Vorlage von Doppelmeldungen zu vermeiden, beispielsweise durch Konsultation öffentlich zugänglicher Schwachstellendatenbanken, projektspezifischer Sicherheits-Beratungsplattformen oder etablierter Problemverfolgungssysteme.

224. Die Hersteller sind verpflichtet, im vorgelagerten Bereich nur jene Schwachstellen zu melden, die in der integrierten Komponente selbst vorhanden sind, und nicht die Schwachstellen, die aufgrund der Integration zwischen der Komponente und einem anderen vom Hersteller entwickelten Code oder aufgrund der Integration anderer Komponenten bestehen. Es kann jedoch Situationen geben, in denen die Integration einer Komponente in ein bestimmtes Produkt mit digitalen Elementen bestimmte Verhaltensweisen, Interaktionen oder sicherheitsrelevante Merkmale dieser Komponente offenbart, die für sich genommen nicht offensichtlich oder nicht leicht identifizierbar waren. In solchen Fällen sind die Hersteller aufgefordert, diese Informationen an jene Person oder Einrichtung zu übermitteln, die die Komponente herstellt oder wartet, um bewährte Verfahren zur Behandlung von Schwachstellen zu fördern, die darauf abzielen, eine wirksame Abhilfe zu erleichtern und die Gesamtsicherheit des Komponentenökosystems zu verbessern.

225. Schließlich sind die Hersteller auch nicht verpflichtet, die Schwachstelle vorgelagert zu melden, wenn für die Komponente kein Wartungsbetrieb mehr zur Verfügung steht oder wenn der Hersteller im Zusammenhang mit neuen Versionen oder Sicherheits-Patches nicht mehr mit dem ursprünglichen Wartungsbetrieb zusammenarbeitet. In solchen Fällen ist der Hersteller dennoch aufgefordert, die Nutzer dieser Komponente durch angemessene alternative Maßnahmen zu informieren, beispielsweise durch bestehende Gemeinschaftsmechanismen (wie etwa Mailinglisten oder die Ausstellung von Tickets) oder durch öffentlich zugängliche Aufzeichnungen über Schwachstellen.

226. Darüber hinaus sind Hersteller, die eine Softwareänderung entwickelt haben, um eine Schwachstelle in einer integrierten Komponente zu behandeln, nach Artikel 13 Absatz 6 verpflichtet, diese Softwareänderung („Sicherheits-Patch“) an die Person oder Einrichtung weiterzugeben, die die Komponente herstellt oder wartet (im Folgenden „vorgelagerte Weitergabe“).

227. Sind Hersteller gemäß Artikel 13 Absatz 6 verpflichtet, einen Sicherheits-Patch zu teilen, so sollte dieser gegebenenfalls in einem maschinenlesbaren Format in einer Weise bereitgestellt werden, die leicht überprüft und gegebenenfalls von der Person oder Einrichtung, die die Komponente herstellt oder wartet, integriert werden kann. Handelt es sich bei der Komponente um eine freie und quelloffene Komponente, so sollte der Sicherheits-Patch in einer Weise geteilt werden, die mit der Lizenz für diese Komponente vereinbar ist, beispielsweise indem sie im Rahmen derselben Lizenz oder einer Lizenz geteilt wird, die es dem Wartungsbetrieb ermöglicht, den Patch im Rahmen seiner eigenen Lizenz zu vertreiben. Verfügt der Wartungsbetrieb dieser Komponente über Leitlinien für das Teilen von Sicherheits-Patches, so sollte der Hersteller diese Leitlinien befolgen.

228. Die Hersteller sind jedoch im Rahmen der Cyberresilienzverordnung nicht verpflichtet, sicherzustellen, dass ihre Sicherheits-Patches notwendigerweise von der Person oder Einrichtung akzeptiert werden, die die Komponente herstellt oder wartet. Sie sind auch nicht verpflichtet, dafür zu sorgen, dass diese Patches notwendigerweise in das Code-Repository der Komponente integriert werden, beispielsweise wenn der Wartungsbetrieb möglicherweise eine andere Option zur Problembehebung bevorzugt. Ebenso sind die Hersteller nicht verpflichtet, einen vom Wartungsbetrieb der Komponente entwickelten, vorgeschlagenen Patch zu akzeptieren, und können es vorziehen, das Problem auf andere geeignete Weise zu mindern.

229. In einigen Fällen ist es möglich, dass die Person oder Einrichtung, die die Komponente herstellt oder wartet, bereits einen Sicherheits-Patch zur Behebung der Schwachstelle bereitgestellt hat, ein Hersteller aber eine andere Minderungsstrategie umsetzt (beispielsweise durch Änderung einer anderen Konfiguration). In solchen Fällen ist der Hersteller gemäß der Cyberresilienzverordnung nicht verpflichtet, die Änderung eines anderen vorgelagerten Teils des Systems zu teilen. Der Hersteller ist dennoch aufgefordert, dies zu tun, wenn dies die Person oder Einrichtung, die die Komponente wartet, unterstützen kann.

9.2.2. *Bekannte ausnutzbare Schwachstellen*

230. Eine der grundlegenden Anforderungen in Anhang I Teil I der Cyberresilienzverordnung sieht vor, dass Produkte mit digitalen Elementen auf Grundlage der in Artikel 13 Absatz 2 genannten Bewertung der Cybersicherheitsrisiken und ohne bekannte ausnutzbare Schwachstellen auf dem Markt bereitgestellt werden müssen.

231. In Artikel 3 Nummer 41 ist eine „ausnutzbare Schwachstelle“ definiert als „eine Schwachstelle, die von einem unbefugten Dritten unter praktischen Betriebsbedingungen wirksam genutzt werden kann“. Unter praktischen Betriebsbedingungen sind nicht alle Schwachstellen ausnutzbar, und es ist möglich, dass einige Schwachstellen nur unter theoretischen Bedingungen (beispielsweise in einem Labor oder in einer Simulation) und/oder nicht unter Bedingungen ausgenutzt werden können, die in der Betriebsumgebung eines Produkts mit digitalen Elementen auftreten würden.

232. Gemäß der Cyberresilienzverordnung müssen die Hersteller über geeignete Strategien und Verfahren verfügen, um potenzielle Schwachstellen, die von internen oder externen Quellen gemeldet werden, zu behandeln und zu beheben (Artikel 13 Absatz 8). Es ist jedoch nicht ausdrücklich festgelegt, wann davon ausgegangen werden sollte, dass eine ausnutzbare Schwachstelle dem Hersteller bekannt ist, wodurch die Verpflichtung entsteht, diese grundlegende Anforderung zum Zeitpunkt des Inverkehrbringens zu erfüllen.

233. Eine Schwachstelle sollte als bekannt gelten, wenn sie in einschlägigen öffentlich zugänglichen Schwachstellendatenbanken wie der gemäß Artikel 12 Absatz 2 der Richtlinie (EU) 2022/2555 eingerichteten europäischen Schwachstellendatenbank oder anderen wichtigen Schwachstellendatenbanken aufgeführt ist.

234. Darüber hinaus kann eine Schwachstelle auch dann bekannt sein, wenn der Hersteller durch nicht öffentliche Informationen darauf aufmerksam gemacht wurde, beispielsweise durch eine koordinierte Offenlegung durch einen Forscher im Bereich der Informationssicherheit oder durch eigene interne Tests und Analysen des Herstellers, beispielsweise bei der Nutzung KI-gestützter Dienste. Ebenso kann eine Schwachstelle bekannt sein, wenn sie öffentlich und an prominenter Stelle in zuverlässigen Medien, beispielsweise in Fachmedien zur Cybersicherheit oder allgemeinen Massenmedien, gemeldet wurde.

235. Die bloße Tatsache, dass eine Schwachstelle gemeldet oder festgestellt wird, bedeutet jedoch für sich genommen nicht, dass sie in der Praxis ausnutzbar oder auf das betreffende Produkt mit digitalen Elementen anwendbar ist. Der Hersteller muss dies untersuchen und die Richtigkeit dieser Informationen sowie die Anwendbarkeit auf sein eigenes Produkt mit digitalen Elementen bestätigen. Dementsprechend kann zwischen der ersten Meldung der Schwachstelle und ihrer Bestätigung ein begrenzter Zeitraum liegen. Wie in Abschnitt *9.1 Meldepflichten* dargelegt, sollte der Schwerpunkt auf raschen Ermittlungs- und Reaktionsmaßnahmen liegen.

236. Darüber hinaus gilt die für Hersteller bestehende Verpflichtung zur Einhaltung der in Anhang I Teil I enthaltenen grundlegenden Anforderungen gemäß Artikel 13 Absatz 1 zum Zeitpunkt des Inverkehrbringens. In der Praxis kann es vorkommen, dass neue potenziell ausnutzbare Schwachstellen in den letzten Phasen des Entwicklungslebenszyklus des Produkts mit digitalen Elementen entdeckt werden, auch kurz vor seinem Eintreten in die Vertriebskette (und damit seinem Inverkehrbringen).

237. Da die Verpflichtung, Produkte mit digitalen Elementen ohne bekannte ausnutzbare Schwachstellen in den Verkehr zu bringen, eine risikobasierte Verpflichtung ist, obliegt es dem Hersteller, auf der Grundlage der Bewertung der Cybersicherheitsrisiken festzustellen, ob das Produkt mit digitalen Elementen im Einklang mit der Cyberresilienzverordnung sicher in den Verkehr gebracht werden kann. Alternativ kann der Hersteller festlegen, dass eine neue Schwachstelle, die bekannt geworden sein könnte, behoben werden muss, bevor das Produkt mit digitalen Elementen in den Verkehr gebracht werden kann. Bei dieser Festlegung sollten die Hersteller die Schwere, die Ausnutzbarkeit und die potenziellen Auswirkungen der Schwachstelle sowie die Risiken berücksichtigen, die sich ab der Verwendung des Produkts mit digitalen Elementen selbst ergeben. Sie können auch das Risiko berücksichtigen, dass die Freigabe des Produkts verschoben wird, bis die Schwachstelle behoben ist, beispielsweise weil die neue Version auch andere ausnutzbare Schwachstellen behebt oder für den weiteren Betrieb kritischer Systeme erforderlich ist. Sobald ein Produkt mit digitalen Elementen in den Verkehr gebracht wurde, bleibt der Hersteller in jedem Fall verpflichtet, Schwachstellen wirksam und im Einklang mit den Anforderungen an die Behandlung von Schwachstellen gemäß Anhang I Teil II zu behandeln.

9.2.3. *Wirksame und regelmäßige Tests und Überprüfungen*

238. Gemäß Anhang I Teil II Nummer 3 müssen die Hersteller während des gesamten Unterstützungszeitraums wirksame und regelmäßige Tests und Überprüfungen des Produkts mit digitalen Elementen durchführen. Für die Durchführung regelmäßiger Tests ist es nicht erforderlich, dass eine unveränderte Testkampagne in festgelegten Zeitabständen mechanisch wiederholt wird. Dies bedeutet, dass regelmäßig überprüft wird, ob neue Informationen, wie neu festgestellte Bedrohungen oder neu entdeckte Schwachstellen, eine Aktualisierung der bestehenden Tests und ein entsprechendes Durchführen dieser Tests erfordern.

239. Häufigkeit, Tiefe und Inhalt der Überprüfung sollten in einem angemessenen Verhältnis zum Cybersicherheitsrisikoprofil des Produkts mit digitalen Elementen, seiner Entwicklung im Laufe der Zeit und der Bedrohungslage stehen. Werden bei der Überprüfung relevante neue Informationen ermittelt, die sich auf die Testkonstellation auswirken, sollten neue oder geänderte Tests entwickelt und an dem Produkt durchgeführt werden, um sicherzustellen, dass keine unbehandelten Schwachstellen verbleiben. Dies kann die erneute Durchführung bestehender Tests umfassen, wenn eine Änderung des Produkts mit digitalen Elementen solche Arten von Tests, wie beispielsweise Regressionstests, angemessen werden lässt.

240. Werden bei der Überprüfung keine solchen Informationen festgestellt, müssen keine zusätzlichen Tests entwickelt werden. Andere Pflichten zur Behandlung von Schwachstellen, einschließlich der Verpflichtung, Schwachstellen im Verhältnis zu den bestehenden Risiken anzugehen und zu beheben, gelten weiterhin parallel.

9.3. **Zusammenwirken mit anderen Rechtsvorschriften**

9.3.1. *Verordnung (EU) 2019/2144 und Verordnung (EU) Nr. 168/2013*

241. In Artikel 2 Absatz 2 Buchstabe c der Cyberresilienzverordnung ist festgelegt, dass die Verordnung nicht für Produkte mit digitalen Elementen gilt, auf welche die Verordnung (EU) 2019/2144 Anwendung findet. Die Verordnung (EU) 2019/2144 gilt für „Fahrzeuge der Klassen M, N und O im Sinne des Artikels 4 der Verordnung (EU) 2018/858 und für Systeme, Bauteile und selbstständige technische Einheiten, die für solche Fahrzeuge konstruiert und gebaut werden".

242. Ebenso wurden Produkte mit digitalen Elementen, die in den Anwendungsbereich der Verordnung (EU) Nr. 168/2013 fallen, durch die Delegierte Verordnung (EU) 2025/1535 der Kommission vom Anwendungsbereich der Cyberresilienzverordnung ausgenommen. Die Verordnung (EU) Nr. 168/2013 gilt für Fahrzeuge der Klasse L und „für Systeme, Bauteile und selbstständige technische Einheiten sowie für Teile und Ausrüstungen, die für solche Fahrzeuge ausgelegt und gebaut werden" (Artikel 2 Absatz 1).

243. Fahrzeuge, auf die diese Bestimmungen anwendbar sind, unterliegen nicht der Cyberresilienzverordnung. Darüber hinaus sind zusätzliche Klarstellungen in Bezug auf den Anwendungsbereich der Ausnahme für Systeme, Komponenten, separate technische Einheiten, Teile und Ausrüstungen (für die Zwecke dieses Abschnitts „Komponenten"), die für solche Fahrzeuge konstruiert und gebaut wurden, die als Produkte mit digitalen Elementen im Sinne der Cyberresilienzverordnung gelten, erforderlich.

244. Es wird davon ausgegangen, dass solche Komponenten nicht der Cyberresilienzverordnung unterliegen, sofern sie ausschließlich für den Einbau in Fahrzeuge ausgelegt und gebaut sind, die unter die Verordnungen (EU) 2019/2144 und (EU) Nr. 168/2013 fallen. Dies gilt unabhängig davon, ob der Hersteller der betreffenden Komponente diese direkt an den Fahrzeughersteller oder an einen anderen Wirtschaftsteilnehmer in der Lieferkette der Automobilindustrie verkauft, sofern die Komponente eindeutig nur für die endgültige Integration in diese Fahrzeuge bestimmt und geeignet ist.

245. Dagegen unterliegt ein Hersteller, der generische Komponenten verkauft, bei denen es sich um Produkte mit digitalen Elementen handelt, die in verschiedene Arten von Produkten und nicht ausschließlich in Fahrzeuge integriert werden können, die unter diese Verordnungen fallen, der Cyberresilienzverordnung.

246. Die Beurteilung, ob eine Komponente im Sinne der Cyberresilienzverordnung in den Verkehr gebracht wird, muss sich auf die objektiven Bedingungen stützen, unter denen sie bereitgestellt wird. Bietet ein Hersteller über Vertriebskanäle, die Kunden außerhalb der Lieferkette der Automobilindustrie offenstehen, wie beispielsweise allgemeine Verkaufsstellen oder Online-Vertriebskanäle, die Bestellungen der breiten Öffentlichkeit entgegennehmen, eine Komponente an, die nicht ausschließlich für die endgültige Integration in diese Fahrzeuge geeignet ist, fällt diese Komponente unabhängig von etwaigen Aussagen über ihre bestimmungsgemäße Verwendung in den Anwendungsbereich der Cyberresilienzverordnung. Unter diesen Umständen kann die Komponente nicht als ausschließlich für den Einbau in Fahrzeuge, die den Verordnungen (EU) 2019/2144 und (EU) Nr. 168/2013 unterliegen, konstruiert und gebaut angesehen werden, und der Hersteller muss die Cyberresilienzverordnung einhalten. Dagegen kann die Nutzung beschränkter Vertriebskanäle zwischen Unternehmen, die auf die Lieferkette der Automobilindustrie beschränkt sind, darauf hindeuten, dass sie ausschließlich für eine solche Integration konzipiert und gebaut wurden.

9.3.2. *Gültigkeit von EU-Baumusterprüfbescheinigungen (Artikel 69 Absatz 1)*

247. In Artikel 69 Absatz 1 der Cyberresilienzverordnung ist Folgendes festgelegt: „EU-Baumusterprüfbescheinigungen und Zulassungen, die in Bezug auf Cybersicherheitsanforderungen für Produkte mit digitalen Elementen erteilt wurden, die anderen Harmonisierungsrechtsvorschriften der Union als der vorliegenden Verordnung unterliegen, bleiben bis zum 11. Juni 2028 gültig, sofern sie nicht vor diesem Zeitpunkt ablaufen oder sofern in anderen Harmonisierungsrechtsvorschriften der Union nichts anderes festgelegt ist; in letzterem Fall bleiben sie gemäß den letztgenannten Rechtsvorschriften gültig".

248. Die weitere Gültigkeit solcher Prüfbescheinigungen und Zulassungen sollte so verstanden werden, dass sie sich auf die Cybersicherheitsrisiken und die entsprechenden Anforderungen beschränkt, die unter jene Harmonisierungsrechtsvorschriften der Union fallen, auf deren Grundlage sie ausgestellt wurden. In Bezug auf diese Risiken sind die Hersteller während der in Artikel 69 Absatz 1 genannten Gültigkeitsdauer für Produkte mit digitalen Elementen, die sie am oder nach dem 11. Dezember 2027 und bis zum 11. Juni 2028 in den Verkehr bringen wollen, nicht verpflichtet, die Konformität ausschließlich für die Zwecke der Cyberresilienzverordnung neu zu bewerten oder erneut nachzuweisen ([31]). Dies ist der Fall bei Prüfbescheinigungen und Zulassungen, die ausgestellt werden, wenn der Hersteller nach den geltenden Harmonisierungsrechtsvorschriften der Union verpflichtet ist, das Konformitätsbewertungsverfahren über eine notifizierte Stelle durchzuführen, und wenn der Hersteller sich freiwillig dafür entschieden hat.

249. Dementsprechend entbindet das Vorliegen einer gültigen Prüfbescheinigung oder Zulassung im Rahmen anderer Harmonisierungsrechtsvorschriften der Union die Hersteller nicht von der Durchführung einer umfassenden Bewertung der Cybersicherheitsrisiken im Rahmen der Cyberresilienzverordnung (und auch nicht von anderen Verpflichtungen im Rahmen dieser Verordnung). Stattdessen können sie sich bei ihrem Konformitätsbewertungsverfahren auf bestehende Prüfbescheinigungen als Nachweis für die Konformität stützen, soweit die entsprechenden Cybersicherheitsrisiken bereits abgedeckt sind. Ist die Prüfbescheinigung oder Zulassung nach anderen Harmonisierungsrechtsvorschriften der Union gültig, die über den 11. Juni 2028 hinaus gelten, so kann sich der Hersteller für die Zwecke der Cyberresilienzverordnung dennoch nur bis zum 11. Juni 2028 auf diese Prüfbescheinigung oder Zulassung berufen.

250. Werden bei der gemäß Artikel 13 Absatz 2 durchgeführten Bewertung der Cybersicherheitsrisiken zusätzliche Risiken festgestellt, die nicht von den Cybersicherheitsanforderungen abgedeckt sind, die der bestehenden Prüfbescheinigung oder Zulassung zugrunde liegen, so bleiben die Hersteller für die Behandlung dieser Risiken im Einklang mit der Cyberresilienzverordnung verantwortlich. In solchen Fällen erfordert die Rechtsbefolgung, dass die festgestellten Lücken bewertet und behoben werden, unabhängig davon, ob die bestehende Prüfbescheinigung oder Zulassung weiterhin gültig ist.

251. Dies lässt sich anhand des Falls veranschaulichen, in dem ein Produkt mit digitalen Elementen den Cybersicherheitsanforderungen der Delegierten Verordnung (EU) 2022/30 der Kommission zur Ergänzung der Richtlinie 2014/53/EU (delegierter Rechtsakt zur Funkanlagenrichtlinie) unterliegt und in dem auf der Grundlage dieser Anforderungen eine EU-Baumusterprüfbescheinigung oder eine Zulassung ausgestellt wurde. In diesem Fall bleibt die Prüfbescheinigung oder die Zulassung gemäß Artikel 69 Absatz 1 für die Cybersicherheitsrisiken gültig, die davon abgedeckt sind und sich auf die grundlegenden Cybersicherheitsanforderungen der Richtlinie 2014/53/EU (Funkanlagenrichtlinie) beziehen.

252. In solchen Fällen sind die Hersteller für die Zwecke der Cyberresilienzverordnung nicht verpflichtet, die Konformität in Bezug auf die Risiken, die bereits durch diese Prüfbescheinigungen abgedeckt sind, neu zu bewerten oder erneut nachzuweisen, solange die entsprechende Prüfbescheinigung oder Zulassung gültig ist, in jedem Fall aber nicht über den 11. Juni 2028 hinaus. Dazu gehören beispielsweise Cybersicherheitsrisiken im Zusammenhang mit dem Schutz von Netzen, dem Schutz personenbezogener Daten und der Privatsphäre oder der Betrugsprävention (soweit diese Risiken durch diese Prüfbescheinigung abgedeckt sind) im Zusammenhang mit den Cybersicherheitsanforderungen der Funkanlagenrichtlinie, die sich in der Konformitätsbewertung widerspiegeln.

253. Werden bei der gemäß Artikel 13 Absatz 2 der Cyberresilienzverordnung durchgeführten Bewertung der Cybersicherheitsrisiken jedoch zusätzliche Cybersicherheitsrisiken festgestellt, die nicht durch diese Prüfbescheinigungen abgedeckt sind, bleiben die Hersteller für die Behandlung dieser Risiken gemäß der Cyberresilienzverordnung verantwortlich. Dies kann beispielsweise Risiken im Zusammenhang mit Verfahren zur Behandlung von Schwachstellen, Datenminimierung und eine Verringerung der Angriffsfläche oder andere produktspezifische Cybersicherheitsaspekte umfassen, die in diesen Prüfbescheinigungen nicht behandelt werden oder in jedem Fall nicht unter die grundlegenden Cybersicherheitsanforderungen der Funkanlagenrichtlinie fallen.

254. Dementsprechend ist das Vorliegen einer gültigen EU-Baumusterprüfbescheinigung oder Zulassung gemäß der Funkanlagenrichtlinie für ihre grundlegenden Anforderungen an die Cybersicherheit für sich genommen kein Nachweis für die vollständige Einhaltung der Cyberresilienzverordnung. Stattdessen ermöglicht sie den Herstellern, sich auf diese Prüfbescheinigung oder Zulassung als Konformitätsnachweis in Bezug auf die entsprechenden Risiken zu stützen, und stellt gleichzeitig sicher, dass alle verbleibenden oder neu ermittelten Risiken im Einklang mit der Cyberresilienzverordnung bewertet und gemindert werden.

([31]) Produkte mit digitalen Elementen, die vor dem 11. Dezember 2027 in den Verkehr gebracht wurden, unterliegen den zum Zeitpunkt ihres Inverkehrbringens geltenden Rechtsvorschriften der Union und können, sofern sie konform sind, verkauft und in Betrieb genommen werden, es sei denn, sie werden am oder nach dem 11. Dezember 2027 wesentlichen Änderungen unterzogen. Zu den Begriffen „Inverkehrbringen“ und „Bereitstellung auf dem Markt“ siehe auch Abschnitt *2.1 Inverkehrbringen* dieses Dokuments sowie Kapitel 2 des „Blue Guide“.

255. Ebenso bleibt in Fällen, in denen ein Produkt mit digitalen Elementen den grundlegenden Sicherheits- und Gesundheitsschutzanforderungen der Verordnung (EU) 2023/1230 (im Folgenden „Maschinenverordnung“) unterliegt, die ab dem 20. Januar 2027 in vollem Umfang gilt, und in denen auf der Grundlage dieser Anforderungen eine EU-Baumusterprüfbescheinigung oder Zulassung ausgestellt wurde, diese Prüfbescheinigung oder Zulassung gemäß Artikel 69 Absatz 1 der Cyberresilienzverordnung für die unter die Maschinenverordnung fallenden Cybersicherheitsrisiken gültig.

256. Dies betrifft insbesondere Cybersicherheitsaspekte im Zusammenhang mit dem Schutz vor Korruption und der Sicherheit und Zuverlässigkeit von Steuerungssystemen, wie in Anhang III Abschnitte 1.1.9 und 1.2.1 der Maschinenverordnung dargelegt. In Bezug auf diese Risiken sind die Hersteller für die Zwecke der Cyberresilienzverordnung nicht verpflichtet, die Konformität erneut zu bewerten oder nachzuweisen, solange die entsprechende Prüfbescheinigung oder Zulassung gültig ist und keinesfalls über den 11. Juni 2028 hinaus. Dies gilt insofern, als die betreffenden Risiken im Rahmen der Konformitätsbewertung nach der Maschinenverordnung behandelt wurden.

257. Werden bei der gemäß Artikel 13 Absatz 2 der Cyberresilienzverordnung durchgeführten Bewertung der Cybersicherheitsrisiken zusätzliche Cybersicherheitsrisiken festgestellt, die nicht durch die einschlägige, gemäß der Maschinenverordnung ausgestellte Prüfbescheinigung abgedeckt sind und die mit den Cybersicherheitsanforderungen der genannten Verordnung im Zusammenhang stehen, so bleiben die Hersteller dafür verantwortlich, diesen Risiken im Einklang mit der Cyberresilienzverordnung zu begegnen – wie vorstehend in Bezug auf die grundlegenden Anforderungen der Funkanlagenrichtlinie zur Cybersicherheit dargelegt.