**Europäisches Parlament**
2019-2024

*Ausschuss für Industrie, Forschung und Energie*

**2022/0272(COD)**

31.3.2023

# ***I
# ENTWURF EINES BERICHTS

zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen an Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020
(COM(2022)0454 - C9-0308/2022 - 2022/0272(COD))

Ausschuss für Industrie, Forschung und Energie

Berichterstatterin: Nicola Danti

## *Symbole für Verfahren*

*Konsultationsverfahren
***Zustimmungsverfahren
***IOrdentliches Gesetzgebungsverfahren (erste Lesung)
***IIOrdentliches Gesetzgebungsverfahren (zweite Lesung)
***IIIOrdentliches Gesetzgebungsverfahren (dritte Lesung)

(Die Art des Verfahrens hängt von der im Gesetzentwurf vorgeschlagenen Rechtsgrundlage ab).

## *Änderungen an einem Entwurf eines Rechtsakts*

**Die Abänderungen des Parlaments sind in zwei Spalten aufgeführt**

Streichungen sind in der linken Spalte ***fett und kursiv*** dargestellt. Ersetzungen sind in beiden Spalten ***fett und kursiv dargestellt***. Neuer Text wird in der rechten Spalte kursiv und ***fett dargestellt***.

In der ersten und zweiten Zeile der Überschrift eines jeden Änderungsantrags wird der betreffende Teil des zu prüfenden Entwurfs eines Rechtsakts angegeben. Bezieht sich ein Änderungsantrag auf einen bestehenden Rechtsakt, der durch den Entwurf eines Rechtsakts geändert werden soll, so enthält die Überschrift des Änderungsantrags eine dritte Zeile, in der der bestehende Rechtsakt genannt wird, und eine vierte Zeile, in der die Bestimmung dieses Rechtsakts genannt wird, die das Parlament ändern möchte.

**Abänderungen des Parlaments in Form eines konsolidierten Textes**

Neuer Text ist durch ***Fett- und Kursivdruck*** hervorgehoben. Streichungen werden entweder durch das ▌ Symbol oder durch Durchstreichen gekennzeichnet. Ersetzungen werden durch Hervorhebung des neuen Textes in ***fetter Kursivschrift*** und durch Streichung oder Durchstreichung des ersetzten Textes gekennzeichnet.
Ausnahmsweise werden rein technische Änderungen, die von den redaktionellen Dienststellen bei der Ausarbeitung des endgültigen Textes vorgenommen wurden, nicht hervorgehoben.

**INHALT**

**Seite**

## ENTWURF EINER LEGISLATIVEN ENTSCHLIESSUNG DES EUROPÄISCHEN PARLAMENTS

**zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen an Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020**
**(COM(2022)0454 - C9-0308/2022 - 2022/0272(COD))**

**(Ordentliches Gesetzgebungsverfahren: erste Lesung)**

*Das Europäische Parlament*,

– gestützt auf den Vorschlag der Kommission an das Parlament und den Rat (KOM(2022)0454),

– gestützt auf Artikel 294 Absatz 2 und Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union, auf deren Grundlage ihm der Vorschlag der Kommission unterbreitet wurde (C9-0308/2022),

– gestützt auf Artikel 294 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union,

– gestützt auf die Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses vom 14. Dezember [20221],

– gestützt auf Artikel 59 seiner Geschäftsordnung,

– unter Hinweis auf die Stellungnahmen des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres und des Ausschusses für Binnenmarkt und Verbraucherschutz,

– unter Hinweis auf den Bericht des Ausschusses für Industrie, Forschung und Energie (A9-0000/2023),

1. legt seinen Standpunkt in erster Lesung fest, der im Folgenden dargelegt wird;

2. fordert die Kommission auf, den dem Vorschlag beigefügten Finanzbogen dahingehend zu ändern, dass der Stellenplan der Agentur der Europäischen Union für Cybersicherheit (ENISA) um 8,5 zusätzliche Vollzeitstellen aufgestockt und entsprechende zusätzliche Mittel bereitgestellt werden, um sicherzustellen, dass die Verpflichtungen der ENISA im Rahmen dieser Verordnung erfüllt werden können und bestehende Verpflichtungen der Agentur im Rahmen anderer Rechtsvorschriften der Union nicht beeinträchtigt werden;

3. fordert die Kommission auf, das Parlament erneut zu befassen, falls sie ihren Vorschlag ersetzt, entscheidend ändert oder beabsichtigt, ihn entscheidend zu ändern;

4. beauftragt seinen Präsidenten, den Standpunkt des Parlaments dem Rat, der Kommission und den nationalen Parlamenten zu übermitteln.

[1] ABl. C 100 vom 16.3.2023, S. 101.

**Abänderung 1**

**Vorschlag für eine**
**Verordnung**
**Erwägungsgrund 1**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (1) Es ist notwendig, das Funktionieren des Binnenmarkts zu verbessern, indem ein einheitlicher Rechtsrahmen für grundlegende Cybersicherheitsanforderungen für das Inverkehrbringen von Produkten mit digitalen Elementen auf dem Unionsmarkt festgelegt wird. Zwei große Probleme, die für die Nutzer und die Gesellschaft mit zusätzlichen Kosten verbunden sind, sollten angegangen werden: ein niedriges Cybersicherheitsniveau von Produkten mit digitalen Elementen, das sich in weit verbreiteten Schwachstellen und der unzureichenden und uneinheitlichen Bereitstellung von Sicherheitsupdates zur Behebung dieser Schwachstellen widerspiegelt, und ein unzureichendes Verständnis und unzureichender Zugang zu Informationen seitens der Nutzer, was sie daran hindert, Produkte mit angemessenen Cybersicherheitseigenschaften auszuwählen oder sie auf sichere Weise zu nutzen. | (1) ***Die Cybersicherheit ist eine der größten Herausforderungen für die Union, und die Zahl und Vielfalt der vernetzten Geräte wird in den kommenden Jahren exponentiell zunehmen. Auch Cyberangriffe sind auf dem Vormarsch und haben nicht nur kritische Auswirkungen auf die Wirtschaft der Union, sondern auch auf die Demokratie und die Gesellschaft in der Union.*** Es ist ***daher*** notwendig, ***das Konzept der Union für die Cybersicherheit und die Widerstandsfähigkeit gegenüber Cyberangriffen zu stärken und*** das Funktionieren des Binnenmarktes zu verbessern, indem ein einheitlicher Rechtsrahmen für die grundlegenden Cybersicherheitsanforderungen für das Inverkehrbringen von Produkten mit digitalen Elementen auf dem Unionsmarkt festgelegt wird. Zwei große Probleme, die den Nutzern und der Gesellschaft zusätzliche Kosten verursachen, sollten angegangen werden: ein niedriges Cybersicherheitsniveau von Produkten mit digitalen Elementen, das sich in weit verbreiteten Schwachstellen und der unzureichenden und uneinheitlichen Bereitstellung von Sicherheitsupdates zur Behebung dieser Schwachstellen widerspiegelt, und ein unzureichendes Verständnis und ein unzureichender Zugang zu Informationen seitens der Nutzer, was sie daran hindert, Produkte mit angemessenen Cybersicherheitseigenschaften auszuwählen oder sie auf sichere Weise zu nutzen. |

Oder. en

**Abänderung 2**

**Vorschlag für eine**
**Verordnung**
**Erwägungsgrund 2**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (2) Ziel dieser Verordnung ist es, die Rahmenbedingungen für die Entwicklung sicherer Produkte mit digitalen Elementen festzulegen, indem | (2) Ziel dieser Verordnung ist es, die Rahmenbedingungen für die Entwicklung sicherer Produkte mit digitalen Elementen festzulegen, indem |

| | |
|---|---|
| Es soll sichergestellt werden, dass Hardware- und Softwareprodukte mit weniger Schwachstellen auf den Markt gebracht werden und dass die Hersteller die Sicherheit während des gesamten Lebenszyklus eines Produkts ernst nehmen. Außerdem sollen Bedingungen geschaffen werden, die es den Nutzern ermöglichen, bei der Auswahl und Nutzung von Produkten mit digitalen Elementen die Cybersicherheit zu berücksichtigen. | Gewährleistung, dass Hardware- und Softwareprodukte mit weniger Schwachstellen auf den Markt kommen und dass die Hersteller die Sicherheit während des gesamten Lebenszyklus eines Produkts ernst nehmen. Außerdem sollen Bedingungen geschaffen werden, die es den Nutzern ermöglichen, bei der Auswahl und Nutzung von Produkten mit digitalen Elementen die Cybersicherheit zu berücksichtigen***, indem beispielsweise die Transparenz in Bezug auf die erwartete Lebensdauer der in Verkehr gebrachten Produkte und die Bereitstellung von Sicherheitsupdates verbessert wird***. |

Oder. en

**Abänderung 3**

**Vorschlag für eine**
**Verordnung**
**Erwägungsgrund 4**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (4) Während die bestehenden Rechtsvorschriften der Union für bestimmte Produkte mit digitalen Elementen gelten, gibt es keinen horizontalen Rechtsrahmen der Union, der umfassende Cybersicherheitsanforderungen für alle Produkte mit digitalen Elementen festlegt. Die verschiedenen Rechtsakte und Initiativen, die bisher auf Unions- und auf nationaler Ebene ergriffen wurden, gehen nur teilweise auf die festgestellten Probleme und Risiken im Zusammenhang mit der Cybersicherheit ein, was zu einem Flickenteppich von Rechtsvorschriften im Binnenmarkt führt, die Rechtsunsicherheit sowohl für die Hersteller als auch für die Nutzer dieser Produkte erhöht und die ***Unternehmen*** unnötig belastet, wenn sie eine Reihe von Anforderungen für ähnliche Produktarten erfüllen müssen. Die Cybersicherheit dieser Produkte hat | eine besonders starke grenzüberschreitende Dimension, da die in einem Land hergestellten Produkte häufig von Organisationen und Verbrauchern im gesamten Binnenmarkt verwendet werden. Daher ist es notwendig, diesen Bereich auf Unionsebene zu regeln. Die Regulierungslandschaft der Union sollte durch die Einführung von Cybersicherheitsanforderungen harmonisiert werden |

(4) Während die bestehenden Rechtsvorschriften der Union für bestimmte Produkte mit digitalen Elementen gelten, gibt es keinen horizontalen Rechtsrahmen der Union, der umfassende Cybersicherheitsanforderungen für alle Produkte mit digitalen Elementen festlegt. Die verschiedenen Rechtsakte und Initiativen, die bisher auf Unionsebene und auf nationaler Ebene ergriffen wurden, gehen nur teilweise auf die festgestellten Probleme und Risiken im Zusammenhang mit der Cybersicherheit ein, was zu einem Flickenteppich von Rechtsvorschriften im Binnenmarkt führt, die Rechtsunsicherheit sowohl für die Hersteller als auch für die Nutzer dieser Produkte erhöht und die ***Unternehmen*** unnötig belastet, wenn sie eine Reihe von Anforderungen für ähnliche Produktarten erfüllen müssen. Die Cybersicherheit dieser Produkte hat eine besonders starke grenzüberschreitende Dimension, da die in einem Land hergestellten Produkte häufig von Organisationen und Verbrauchern im gesamten Binnenmarkt verwendet werden. Daher ist es notwendig, diesen Bereich auf Unionsebene zu regeln***, um einen harmonisierten und klaren Rechtsrahmen für Unternehmen zu schaffen, insbesondere***

für Produkte mit digitalen Elementen. Darüber hinaus sollte in der gesamten Union Sicherheit für Betreiber und Nutzer sowie eine bessere Harmonisierung des Binnenmarktes gewährleistet werden, um für Betreiber, die in den EU-Markt eintreten wollen, tragfähigere Bedingungen zu schaffen.

***Kleinst-, kleine und mittlere Unternehmen***. Die Regulierungslandschaft der Union sollte durch die Einführung von Cybersicherheitsanforderungen für Produkte mit digitalen Elementen harmonisiert werden. Darüber hinaus sollte in der gesamten Union Sicherheit für Betreiber und Nutzer sowie eine bessere Harmonisierung des Binnenmarktes gewährleistet werden, um für Betreiber, die in den Unionsmarkt eintreten wollen, bessere Bedingungen zu schaffen.

Oder. en

**Abänderung 4**

**Vorschlag für eine Verordnung Erwägung 4 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(4a) Der horizontale Charakter dieser Verordnung bedeutet, dass sie sich auf sehr unterschiedliche Segmente der Wirtschaft in der Union auswirken wird. Daher ist es wichtig, dass die Besonderheiten der einzelnen Sektoren berücksichtigt werden und dass die in dieser Verordnung festgelegten Cybersicherheitsanforderungen in einem angemessenen Verhältnis zu den Risiken stehen, um eine Überlastung bestimmter Sektoren zu vermeiden. Die Kommission sollte Leitlinien, auch in Bezug auf diese Fragen, herausgeben und veröffentlichen, um die Unternehmen bei der Durchführung dieser Verordnung zu unterstützen.*** |

Oder. en

**Abänderung 5**

**Vorschlag für eine**
**Verordnung**
**Erwägungsgrund 5**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (5) Auf Unionsebene wurden in verschiedenen programmatischen und politischen Dokumenten wie der EU-Cybersicherheitsstrategie für das digitale Jahrzehnt[16], den Schlussfolgerungen des Rates vom 2. Dezember 2020 und vom 23. Mai 2022 oder der Entschließung des Europäischen Parlaments vom 10. Juni 2021[17] spezifische Cybersicherheitsanforderungen der Union für digitale oder vernetzte Produkte gefordert, und mehrere Länder auf der ganzen Welt haben von sich aus Maßnahmen zur Lösung dieses Problems ergriffen. Im Abschlussbericht der Konferenz über die Zukunft Europas[18] forderten die Bürgerinnen und Bürger "eine stärkere Rolle der EU bei der Abwehr von Cybersicherheitsbedrohungen". | (5) Auf Unionsebene wurden in verschiedenen programmatischen und politischen Dokumenten wie der EU-Cybersicherheitsstrategie für das digitale Jahrzehnt[16], den Schlussfolgerungen des Rates vom 2. Dezember 2020 und vom 23. Mai 2022 oder der Entschließung des Europäischen Parlaments vom 10. Juni 2021[17] spezifische Cybersicherheitsanforderungen der Union für digitale oder vernetzte Produkte gefordert, und mehrere Länder auf der ganzen Welt haben aus eigener Initiative Maßnahmen zur Bewältigung dieses Problems eingeführt. Im Abschlussbericht der Konferenz über die Zukunft Europas[18] forderten die Bürger "eine stärkere Rolle der EU bei der Bekämpfung von Cybersicherheitsbedrohungen". Damit ***die Union eine führende internationale Rolle im Bereich der Cybersicherheit spielen kann, muss ein ehrgeiziger übergreifender Rechtsrahmen geschaffen werden.*** |
| [16] JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN. | [16] JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN. |
| [17] 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_EN.html. | [17] 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_EN.html. |
| [18] Konferenz über die Zukunft Europas - Bericht über das Endergebnis, Mai 2022, Vorschlag 28(2). Die Konferenz fand zwischen April 2021 und Mai 2022 statt. Es handelte sich um eine einzigartige, von den Bürgern geleitete Übung der deliberativen Demokratie auf gesamteuropäischer Ebene, an der Tausende von europäischen Bürgern sowie politische Akteure, Sozialpartner, Vertreter der Zivilgesellschaft und wichtige Interessengruppen teilnahmen. | [18] Konferenz über die Zukunft Europas - Bericht über das Endergebnis, Mai 2022, Vorschlag 28(2). Die Konferenz fand zwischen April 2021 und Mai 2022 statt. Es handelte sich um eine einzigartige, von den Bürgern geleitete Übung der deliberativen Demokratie auf gesamteuropäischer Ebene, an der Tausende von europäischen Bürgern sowie politische Akteure, Sozialpartner, Vertreter der Zivilgesellschaft und wichtige Interessengruppen teilnahmen. |

**Abänderung 6**

**Vorschlag für eine**
**Verordnung**
**Erwägungsgrund 8**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (8) Durch die Festlegung von Cybersicherheitsanforderungen für das Inverkehrbringen von Produkten mit digitalen Elementen wird die Cybersicherheit dieser Produkte sowohl für Verbraucher als auch für Unternehmen verbessert. Dies gilt auch für Anforderungen an das Inverkehrbringen von Verbraucherprodukten mit digitalen Elementen, die für gefährdete Verbraucher bestimmt sind, wie Spielzeug und Babyphone. | (8) Durch die Festlegung von Cybersicherheitsanforderungen für das Inverkehrbringen von Produkten mit digitalen Elementen wird die Cybersicherheit dieser Produkte sowohl für Verbraucher als auch für Unternehmen verbessert. Dies gilt auch für Anforderungen an das Inverkehrbringen von Verbraucherprodukten mit digitalen Elementen, die für gefährdete Verbraucher bestimmt sind, wie Spielzeug und Babyphone. ***Diese Anforderungen werden auch sicherstellen, dass die Cybersicherheit in der gesamten Lieferkette b e r ü c k s i c h t i g t wird, um die Sicherheit der Endprodukte mit digitalen Elementen zu erhöhen. Dies wird wiederum einen Wettbewerbsvorteil für die in der Union niedergelassenen oder vertretenen Hersteller darstellen, die so die Cybersicherheit ihrer Produkte nachweisen können.*** |

Oder. en

**Abänderung 7**

**Vorschlag für eine**
**Verordnung**
**Erwägungsgrund 9**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (9) Diese Verordnung gewährleistet ein hohes Maß an Cybersicherheit für Produkte mit digitalen Elementen. Sie regelt keine Dienstleistungen wie Software-as-a-Service (SaaS), mit Ausnahme von Lösungen für die Datenfernverarbeitung im Zusammenhang | mit einem Produkt mit digitalen Elementen, d. h. jede Datenverarbeitung aus der Ferne, für die die Software vom Hersteller des betreffenden Produkts oder unter der Verantwortung dieses Herstellers konzipiert und entwickelt wird |

(9) Diese Verordnung gewährleistet ein hohes Maß an Cybersicherheit für Produkte mit digitalen Elementen. Sie regelt keine Dienstleistungen wie Software-as-a-Service (SaaS), mit Ausnahme von Lösungen für die Datenfernverarbeitung im Zusammenhang mit einem Produkt mit digitalen Elementen, d. h. jede Datenverarbeitung aus der Ferne, für die die Software vom Hersteller des betreffenden Produkts oder unter der Verantwortung dieses Herstellers konzipiert und entwickelt wird

Die Richtlinie XXX/XXXX (NIS2)] legt Anforderungen an die Cybersicherheit und die Meldung von Vorfällen für wesentliche Einrichtungen wie kritische Infrastrukturen fest. Mit der ***[Richtlinie XXX/XXXX (NIS2)]*** werden Anforderungen an die Cybersicherheit und die Meldung von Vorfällen für wesentliche und wichtige Einrichtungen wie kritische Infrastrukturen eingeführt, um die Widerstandsfähigkeit der von ihnen erbrachten Dienste zu erhöhen. Die ***[Richtlinie XXX/XXXX (NIS2)]*** gilt für Cloud-Computing-Dienste und Cloud-Service-Modelle, wie SaaS. Alle Einrichtungen, die in der Union Cloud-Computing-Dienste anbieten und den Schwellenwert für mittlere Unternehmen erreichen oder überschreiten, fallen in den Anwendungsbereich dieser Richtlinie.

und deren Fehlen ein solches Produkt mit digitalen Elementen daran hindern würde, eine seiner Kernfunktionen zu erfüllen. Mit der ***Richtlinie (EU) 2022/2555*** werden Anforderungen an die Cybersicherheit und die Meldung von Vorfällen für wesentliche und wichtige Einrichtungen wie kritische Infrastrukturen eingeführt, um die Widerstandsfähigkeit der von ihnen erbrachten Dienste zu erhöhen. ***Die Richtlinie (EU) 2022/2555*** gilt für Cloud-Computing-Dienste und Cloud-Service-Modelle, wie SaaS. Alle Unternehmen, die in der Union Cloud-Computing-Dienste anbieten und den Schwellenwert für mittlere Unternehmen erreichen oder überschreiten, fallen in den Anwendungsbereich dieser Richtlinie.

Oder. en

**Abänderung 8**

**Vorschlag für eine**
**Verordnung**
**Erwägungsgrund 10**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (10) Um Innovation und Forschung nicht zu behindern, sollte freie und quelloffene Software, die ***außerhalb*** einer gewerblichen Tätigkeit ***entwickelt oder*** bereitgestellt wird, ***nicht*** unter diese Verordnung fallen***. Dies gilt insbesondere für Software, einschließlich ihres Quellcodes und geänderter Versionen, die offen gemeinsam genutzt wird und frei zugänglich, nutzbar, veränderbar und weiterverteilbar ist***. Im Zusammenhang mit Software kann eine kommerzielle Tätigkeit nicht nur durch die Erhebung eines Preises für ein Produkt gekennzeichnet sein, sondern auch durch die Erhebung eines Preises für technische Unterstützungsdienste, durch die Bereitstellung einer Softwareplattform, über die der Hersteller andere Dienste | monetarisiert, oder durch die Verwendung personenbezogener Daten aus anderen Gründen als ausschließlich zur Verbesserung der Sicherheit, Kompatibilität oder Interoperabilität der Software. |

(10) Um Innovation und Forschung nicht zu behindern, sollte ***nur*** freie und quelloffene Software, die ***im Rahmen einer*** gewerblichen Tätigkeit bereitgestellt wird, unter diese Verordnung fallen. Im Zusammenhang mit Software kann eine kommerzielle Tätigkeit nicht nur durch die Erhebung eines Preises für ein Produkt gekennzeichnet sein, sondern auch durch die Erhebung eines Preises für technische Unterstützungsdienste, durch die Bereitstellung einer Softwareplattform, über die der Hersteller andere Dienste monetarisiert, oder durch die Verwendung personenbezogener Daten aus anderen Gründen als ausschließlich zur Verbesserung der Sicherheit, Kompatibilität oder Interoperabilität der Software. ***Wurde freie und quelloffene Software außerhalb einer kommerziellen Tätigkeit entwickelt oder bereitgestellt, sollten Hersteller, die solche Software in ihre Produkte mit digitalen Elementen einbauen, alle erforderlichen Maßnahmen ergreifen, um sicherzustellen, dass die***

***die Einhaltung dieser Verordnung.***

Oder. en

**Abänderung 9**

**Vorschlag für eine Verordnung Erwägung 12 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(12a) Produkte mit digitalen Elementen, die ausschließlich für die nationale Sicherheit oder für militärische Zwecke entwickelt werden, oder Produkte, die speziell für die Verarbeitung von Verschlusssachen konzipiert sind, fallen nicht in den Anwendungsbereich dieser Verordnung. Die Mitgliedstaaten werden jedoch aufgefordert, für diese Produkte das gleiche oder ein höheres Schutzniveau zu gewährleisten wie für Produkte, die in den Geltungsbereich dieser Verordnung fallen.*** |

Oder. en

**Abänderung 10**

**Vorschlag für eine Verordnung Erwägung 14 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(14a) Diese Verordnung sollte nicht für Bauteile gelten, die ausschließlich hergestellt werden, um identische Bauteile bei Reparaturen in älteren Produkten mit digitalen Elementen zu ersetzen, um zu vermeiden, dass Produkte mit digitalen Elementen, die bereits im Binnenmarkt im Umlauf sind, wegen fehlender Ersatzteile aus dem Verkehr gezogen werden müssen.*** |

Oder. en

**Abänderung 11**

**Vorschlag für eine**
**Verordnung Erwägung**
**14 b (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(14b) Leasinggesellschaften gelten nicht als Händler im Sinne dieser Verordnung, sofern ihre Tätigkeit ausschließlich als Finanzierung oder Kreditgewährung zur Unterstützung der Tätigkeit der Hersteller oder anderer Wirtschaftsteilnehmer anzusehen ist.*** |

Oder. en

*Rechtfertigung*

*Leasinggesellschaften, die bei Leasingverträgen zu Finanzierungszwecken als Dritte auftreten, sollten nicht als Händler gelten, sofern sich ihre Tätigkeit ausschließlich auf das Finanzierungselement konzentriert.*

**Abänderung 12**

**Vorschlag für eine**
**Verordnung**
**Erwägungsgrund 15**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (15)Die Delegierte Verordnung (EU) 2022/30 legt fest, dass die grundlegenden Anforderungen gemäß Artikel 3 Absatz 3 Buchstabe d (Schädigung des Netzes und Missbrauch von Netzressourcen), Buchstabe e (personenbezogene Daten und Schutz der Privatsphäre) und Buchstabe f (Betrug) der Richtlinie 2014/53/EU für bestimmte Funkanlagen gelten. Im [Durchführungsbeschluss XXX/2022 der Kommission über einen Normungsauftrag an die europäischen Normungsorganisationen] werden Anforderungen für die Entwicklung spezifischer Normen festgelegt, in denen näher ausgeführt wird, wie diese drei | grundlegenden Anforderungen erfüllt w e r d e n sollten. Die in dieser Verordnung festgelegten grundlegenden Anforderungen umfassen alle Elemente der in Artikel 3 Absatz 3 Buchstaben d und e genannten grundlegenden Anforderungen |

(15)Die Delegierte Verordnung (EU) 2022/30 legt fest, dass die grundlegenden Anforderungen gemäß Artikel 3 Absatz 3 Buchstabe d (Schädigung des Netzes und Missbrauch von Netzressourcen), Buchstabe e (personenbezogene Daten und Schutz der Privatsphäre) und Buchstabe f (Betrug) der Richtlinie 2014/53/EU für bestimmte Funkanlagen gelten. Im [Durchführungsbeschluss XXX/2022 der Kommission über einen Normungsauftrag an die europäischen Normungsorganisationen] werden Anforderungen für die Entwicklung spezifischer Normen festgelegt, in denen näher ausgeführt wird, wie diese drei grundlegenden Anforderungen erfüllt werden sollten. Die in dieser Verordnung festgelegten grundlegenden Anforderungen umfassen alle Elemente der in Artikel 3 Absatz 3 Buchstaben d und e genannten grundlegenden Anforderungen

und Buchstabe f der Richtlinie 2014/53/EU. Darüber hinaus sind die in dieser Verordnung festgelegten grundlegenden Anforderungen auf die Ziele der in diesem Normungsauftrag enthaltenen Anforderungen an spezifische Normen abgestimmt.
Wenn die Kommission die Delegierte Verordnung (EU) 2022/30 aufhebt oder ändert, so dass sie für bestimmte Produkte, die unter diese Verordnung fallen, nicht mehr gilt, sollten die Kommission und die europäischen Normungsorganisationen daher die Normungsarbeit, die im Rahmen des Durchführungsbeschlusses C(2022)5637 der Kommission über einen Normungsauftrag für die Delegierte Verordnung (EU) 2022/30 durchgeführt wurde, bei der Ausarbeitung und Entwicklung harmonisierter Normen berücksichtigen, um die Durchführung dieser Verordnung zu erleichtern.

und Buchstabe f der Richtlinie 2014/53/EU. Darüber hinaus sind die in dieser Verordnung festgelegten grundlegenden Anforderungen auf die Ziele der in diesem Normungsauftrag enthaltenen Anforderungen an spezifische Normen abgestimmt.
Wenn die Kommission die Delegierte Verordnung (EU) 2022/30 aufhebt oder ändert, so dass sie für bestimmte Produkte, die unter diese Verordnung fallen, nicht mehr gilt, sollten die Kommission und die europäischen Normungsorganisationen daher die Normungsarbeiten, die im Rahmen des Durchführungsbeschlusses C(2022)5637 der Kommission über einen Normungsantrag für die Delegierte Verordnung (EU) 2022/30 durchgeführt wurden, bei der Ausarbeitung und Entwicklung harmonisierter Normen berücksichtigen, um die Durchführung dieser Verordnung zu erleichtern. ***Wenn Hersteller diese Verordnung vor ihrem Geltungsbeginn einhalten, wird davon ausgegangen, dass sie auch die Delegierte Verordnung (EU) 2022/30 einhalten, bis die Kommission diese Delegierte Verordnung aufhebt.***

Oder. en

**Abänderung 13**

**Vorschlag für eine Verordnung Erwägung 18 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(18a) Bei der Beschaffung von Produkten mit digitalen Elementen sollten die Mitgliedstaaten Produkten mit einem hohen Maß an Cybersicherheit und einer angemessenen erwarteten Produktlebensdauer den Vorzug geben, um ihre Fähigkeit zur Bewältigung von Cyberbedrohungen zu verbessern und die effiziente Nutzung öffentlicher*** |

***Ressourcen zu gewährleisten. Darüber hinaus sollten die Mitgliedstaaten sicherstellen, dass die Hersteller Schwachstellen, die öffentlich beschaffte Produkte betreffen, mit***

***digitale Elemente dringend erforderlich.***

Oder. en

**Abänderung 14**

**Vorschlag für eine**
**Verordnung**
**Erwägungsgrund 19**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (19) Bestimmte in dieser Verordnung vorgesehene Aufgaben sollten von der ENISA im Einklang mit Artikel 3 Absatz 2 der Verordnung (EU) 2019/881 wahrgenommen werden. Insbesondere sollte die ENISA von den Herstellern Meldungen über aktiv ausgenutzte Sicherheitslücken in Produkten mit digitalen Elementen sowie über Vorfälle mit Auswirkungen auf die Sicherheit dieser Produkte erhalten. Die ENISA sollte diese Meldungen auch an die einschlägigen Computer Security Incident Response Teams (CSIRTs) bzw. an die gemäß Artikel [Artikel X] der ***Richtlinie [Richtlinie XXX / XXXX (NIS2)]*** benannten einheitlichen Ansprechpartner der Mitgliedstaaten weiterleiten und die zuständigen Marktüberwachungsbehörden über die gemeldete Schwachstelle informieren. Auf der Grundlage der von ihr gesammelten Informationen sollte die ENISA alle zwei Jahre einen technischen Bericht über sich abzeichnende Trends in Bezug auf Cybersicherheitsrisiken bei Produkten mit digitalen Elementen erstellen und ihn der in der ***Richtlinie [Richtlinie XXX / XXXX (NIS2)]*** genannten Kooperationsgruppe vorlegen. Darüber hinaus sollte die ENISA in Anbetracht ihres Fachwissens und ihres Mandats in der Lage sein, den Prozess der Durchführung dieser Verordnung zu unterstützen. Insbesondere sollte sie in der Lage sein, gemeinsame Aktivitäten vorzuschlagen, die von den | Marktüberwachungsbehörden auf der Grundlage von Hinweisen oder Informationen über eine mögliche Nichtkonformität von Produkten mit digitalen Elementen mit dieser Verordnung in mehreren Mitgliedstaaten durchgeführt werden. |

(19) Bestimmte in dieser Verordnung vorgesehene Aufgaben sollten von der ENISA im Einklang mit Artikel 3 Absatz 2 der Verordnung (EU) 2019/881 wahrgenommen werden. Insbesondere sollte die ENISA von den Herstellern Meldungen über aktiv ausgenutzte Sicherheitslücken in Produkten mit digitalen Elementen sowie über ***erhebliche*** Vorfälle mit Auswirkungen auf die Sicherheit dieser Produkte erhalten. Die ENISA sollte diese Meldungen auch an die einschlägigen Computer Security Incident Response Teams (CSIRTs) bzw. an die gemäß Artikel [Artikel X] der ***Richtlinie (EU) 2022/2555 benannten*** einheitlichen Ansprechpartner der Mitgliedstaaten weiterleiten und die zuständigen Marktaufsichtsbehörden über die gemeldete Schwachstelle informieren***. Die ENISA sollte sicherstellen, dass solche Meldungen über sichere Kanäle empfangen, gespeichert und übermittelt werden und dass klare Protokolle darüber bestehen, wer auf sie zugreifen kann und welche Vorkehrungen für ihre Weiterleitung getroffen wurden. Die ENISA sollte keine Informationen über Schwachstellen an die Öffentlichkeit weitergeben, für die keine Sicherheitsaktualisierung verfügbar ist***. Auf der Grundlage der von ihr gesammelten Informationen sollte die ENISA alle zwei Jahre einen technischen Bericht über sich abzeichnende Trends in Bezug auf Cybersicherheitsrisiken bei Produkten mit digitalen Elementen erstellen und ihn der in der ***Richtlinie (EU) 2022/2555*** genannten Kooperationsgruppe vorlegen. Darüber hinaus sollte die ENISA in Anbetracht ihres Fachwissens und ihres Mandats in der Lage sein, Folgendes zu unterstützen

| | |
|---|---|
| Festlegung von Produktkategorien, für die gleichzeitige koordinierte Kontrollmaßnahmen organisiert werden sollten. In Ausnahmefällen sollte die ENISA auf Ersuchen der Kommission in der Lage sein, Bewertungen in Bezug auf bestimmte Produkte mit digitalen Elementen durchzuführen, die ein erhebliches Cybersicherheitsrisiko darstellen und bei denen ein sofortiges Eingreifen erforderlich ist, um das reibungslose Funktionieren des Binnenmarkts zu gewährleisten. | das Verfahren zur Durchführung dieser Verordnung. Insbesondere sollte sie in der Lage sein, gemeinsame Maßnahmen vorzuschlagen, die von den Marktüberwachungsbehörden auf der Grundlage von Hinweisen oder Informationen über eine mögliche Nichteinhaltung dieser Verordnung bei Produkten mit digitalen Elementen in mehreren Mitgliedstaaten durchzuführen sind, oder Kategorien von Produkten zu ermitteln, für die gleichzeitige koordinierte Kontrollmaßnahmen organisiert werden sollten. In Ausnahmefällen sollte die ENISA auf Ersuchen der Kommission in der Lage sein, Bewertungen in Bezug auf bestimmte Produkte mit digitalen Elementen durchzuführen, die ein erhebliches Cybersicherheitsrisiko darstellen und bei denen ein sofortiges Eingreifen erforderlich ist, um das reibungslose Funktionieren des Binnenmarkts zu gewährleisten.<br><br>Oder. en |

**Abänderung 15**

**Vorschlag für eine Verordnung Erwägung 19 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(19a) Die ENISA sollte gemeldete Sicherheitslücken in der gemäß der Richtlinie (EU) 2022/2555 eingerichteten europäischen Datenbank für Sicherheitslücken veröffentlichen. Die ENISA sollte über ein geeignetes Verfahren für den Veröffentlichungsprozess verfügen, damit die Hersteller Zeit haben, die erforderlichen Sicherheitsaktualisierungen zu entwickeln, und die Nutzer Zeit haben, diese zu implementieren oder andere Korrektur- oder Abhilfemaßnahmen zu*** |

***ergreifen. Die Datenbank soll den Herstellern helfen, bekannte ausnutzbare Schwachstellen aufzuspüren und ihre Kritikalität zu verstehen, damit sie sicherere Produkte auf den Markt bringen können.***

Oder. en

**Abänderung 16**

**Vorschlag für eine Verordnung Erwägung 27**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (27) Die in Anhang III dieser Verordnung genannten Kategorien kritischer Produkte mit digitalen Elementen sind als die Produkte zu verstehen, die die Kernfunktionalität des in Anhang III dieser Verordnung aufgeführten Typs aufweisen. So sind beispielsweise in Anhang III dieser Verordnung Produkte aufgeführt, die aufgrund ihrer Kernfunktionalität als Allzweck-Mikroprozessoren der Klasse II definiert sind. Infolgedessen unterliegen Mikroprozessoren für allgemeine Zwecke der obligatorischen Konformitätsbewertung durch Dritte. Dies gilt nicht für andere, nicht ausdrücklich in Anhang III dieser Verordnung aufgeführte Produkte, die einen Mikroprozessor für allgemeine Zwecke enthalten können. Die Kommission sollte [innerhalb von ***12 Monaten*** nach Inkrafttreten dieser Verordnung] delegierte Rechtsakte erlassen, um die Definitionen der unter Klasse I und Klasse II fallenden Produktkategorien gemäß Anhang III zu präzisieren. | (27) Die in Anhang III dieser Verordnung genannten Kategorien kritischer Produkte mit digitalen Elementen sind als die Produkte zu verstehen, die die Kernfunktionalität des in Anhang III dieser Verordnung aufgeführten Typs aufweisen. So sind beispielsweise in Anhang III dieser Verordnung Produkte aufgeführt, die aufgrund ihrer Kernfunktionalität als Allzweck-Mikroprozessoren der Klasse II definiert sind. Infolgedessen unterliegen Mikroprozessoren für allgemeine Zwecke der obligatorischen Konformitätsbewertung durch Dritte. Dies gilt nicht für andere, nicht ausdrücklich in Anhang III dieser Verordnung aufgeführte Produkte, die einen Mikroprozessor für allgemeine Zwecke enthalten können. Die Kommission sollte [innerhalb von ***sechs*** Monaten nach Inkrafttreten dieser Verordnung] delegierte Rechtsakte erlassen, um die Definitionen der unter Klasse I und Klasse II fallenden Produktkategorien gemäß Anhang III zu präzisieren. ***Um Rechtsklarheit und -sicherheit zu gewährleisten, sollten Änderungen an der Liste in Anhang III nicht häufiger als alle zwei Jahre vorgenommen und erst nach einer gründlichen Bewertung durch die Kommission, einschließlich einer Konsultation der Interessengruppen, verabschiedet werden.*** |

Oder. en

**Abänderung 17**

**Vorschlag für eine Verordnung Erwägung 27 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(27a) Die Kommission sollte eine Sachverständigengruppe für Cyber-Resilienz (die "Sachverständigengruppe") mit einer breiten und vielfältigen Mitgliedschaft einsetzen. Die Expertengruppe sollte die Kommission unterstützen, um die ordnungsgemäße Durchführung dieser Verordnung zu gewährleisten, indem sie die Kommission beispielsweise zu möglichen Änderungen der Liste kritischer Produkte in Anhang III berät oder analysiert, inwieweit europäische und internationale Normen die Einhaltung der grundlegenden Anforderungen dieser Verordnung ermöglichen können.*** |

Oder. en

**Abänderung 18**

**Vorschlag für eine**
**Verordnung**
**Erwägungsgrund 32**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (32) Um zu gewährleisten, dass Produkte mit digitalen Elementen sowohl zum Zeitpunkt ihres Inverkehrbringens als auch während ihres gesamten Lebenszyklus sicher sind, müssen grundlegende Anforderungen für den Umgang mit Sicherheitslücken und grundlegende Cybersicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen festgelegt werden. Während die Hersteller alle grundlegenden Anforderungen für den Umgang mit Sicherheitslücken einhalten ***und sicherstellen*** sollten***, dass alle ihre Produkte ohne bekannte ausnutzbare Sicherheitslücken ausgeliefert werden***, | sollten sie bestimmen, welche anderen grundlegenden Anforderungen in Bezug auf die Produkteigenschaften für die betreffende Art von Produkt relevant sind. Zu diesem Zweck sollten die Hersteller eine Bewertung der Cybersicherheitsrisiken vornehmen, die mit einem Produkt mit digitalen |

(32) Um zu gewährleisten, dass Produkte mit digitalen Elementen sowohl zum Zeitpunkt ihres Inverkehrbringens als auch während ihres gesamten Lebenszyklus sicher sind, müssen grundlegende Anforderungen für den Umgang mit Sicherheitslücken und grundlegende Cybersicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen festgelegt werden. Die Hersteller sollten zwar alle grundlegenden Anforderungen für den Umgang mit Sicherheitslücken ***während der gesamten voraussichtlichen Lebensdauer des Produkts einhalten***, sie sollten aber auch bestimmen, welche anderen grundlegenden Anforderungen in Bezug auf die Produkteigenschaften für die betreffende Art von Produkt relevant sind. Zu diesem Zweck sollten die Hersteller eine Bewertung der mit einem Produkt mit digitalen Elementen verbundenen Cybersicherheitsrisiken vornehmen, um relevante Risiken und relevante grundlegende Anforderungen zu ermitteln und um

| | |
|---|---|
| Elemente, um relevante Risiken und relevante grundlegende Anforderungen zu ermitteln und um geeignete harmonisierte Normen oder gemeinsame Spezifikationen angemessen anzuwenden. | ***ihre Produkte ohne bekannte ausnutzbare Schwachstellen zu liefern, die sich auf die Sicherheit dieser Produkte auswirken könnten, und*** geeignete harmonisierte Normen oder gemeinsame Spezifikationen angemessen anzuwenden. |

Oder. en

**Abänderung 19**

**Vorschlag für eine Verordnung Erwägung 32 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(32a) Die Hersteller sollten nach Möglichkeit und insbesondere bei Produkten, die von Unternehmen an Verbraucher verkauft werden, dafür sorgen, dass Sicherheitsaktualisierungen automatisch installiert werden, um potenzielle Schwachstellen so bald wie möglich zu beheben. Die Nutzer sollten weiterhin die Möglichkeit haben, diese Funktion zu deaktivieren. Sobald ein Produkt mit digitalen Elementen das Ende seiner voraussichtlichen Lebensdauer erreicht hat und keine Sicherheitsaktualisierungen mehr zur Verfügung gestellt werden, sollten die Hersteller die Nutzer auf einfache und klare Weise informieren, z. B. durch eine benutzerfreundliche Benachrichtigung.*** |

Oder. en

**Abänderung 20**

**Vorschlag für eine Verordnung Erwägung 32 b (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|

***(32b) Wenn Hersteller die voraussichtliche Lebensdauer auf einen kürzeren Zeitraum als fünf Jahre festlegen und daher keine Sicherheitsaktualisierungen für das Produkt mit digitalen Elementen mehr anbieten, sollten sie***

***ihren Quellcode Unternehmen zur Verfügung stellen, die Sicherheitsaktualisierungen und andere ähnliche Dienste anbieten wollen. Ein solcher Zugang sollte nur im Rahmen einer vertraglichen Vereinbarung gewährt werden, die das Eigentum an dem Produkt mit digitalen Elementen schützt und die Verbreitung des Quellcodes an die Allgemeinheit verhindert. Die Verpflichtung, freien Zugang zum Quellcode zu gewähren, sollte nur für fünf Jahre nach dem Inverkehrbringen des Produkts mit digitalen Bestandteilen gelten.***

Oder. en

**Abänderung 21**

**Vorschlag für eine Verordnung**
**Erwägungsgrund 34**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (34) Um sicherzustellen, dass die nationalen CSIRTs und die gemäß Artikel [Artikel X] der ***Richtlinie [Richtlinie XX/XXXX (NIS2)]*** benannten zentralen Anlaufstellen mit den Informationen versorgt werden, die sie zur Erfüllung ihrer Aufgaben und zur Anhebung des allgemeinen Niveaus der Cybersicherheit wesentlicher und wichtiger Einrichtungen benötigen, und um das wirksame Funktionieren der Marktüberwachungsbehörden zu gewährleisten, sollten die Hersteller von Produkten mit digitalen Elementen der ENISA Sicherheitslücken melden, die aktiv ausgenutzt werden. Da die meisten Produkte mit digitalen Elementen im gesamten Binnenmarkt vermarktet werden, sollte jede ausgenutzte Schwachstelle in einem Produkt mit digitalen Elementen als Bedrohung für das Funktionieren des Binnenmarktes angesehen werden. Die | Hersteller sollten ***auch in Erwägung ziehen,*** behobene Schwachstellen in der gemäß der ***Richtlinie [Richtlinie XX/XXXX (NIS2)]*** eingerichteten und von der ENISA verwalteten europäischen Schwachstellendatenbank ***oder in jeder anderen öffentlich zugänglichen Schwachstellendatenbank zu veröffentlichen.*** |

(34) Um sicherzustellen, dass die nationalen CSIRTs und die gemäß Artikel [Artikel X] der ***Richtlinie (EU) 2022/2555*** benannte zentrale Kontaktstelle mit den Informationen versorgt werden, die sie zur Erfüllung ihrer Aufgaben und zur Anhebung des allgemeinen Cybersicherheitsniveaus wesentlicher und wichtiger Einrichtungen benötigen, und um das wirksame Funktionieren der Marktüberwachungsbehörden zu gewährleisten, sollten die Hersteller von Produkten mit digitalen Elementen der ENISA Sicherheitslücken melden, die aktiv ausgenutzt werden. Die ***Meldepflicht sollte nicht für Schwachstellen gelten, die von ethischen Sicherheitshackern entdeckt werden, die ohne böswillige Absicht und mit Zustimmung des Herstellers arbeiten.*** Da die meisten Produkte mit digitalen Elementen im gesamten Binnenmarkt vermarktet werden, sollte jede ausgenutzte Schwachstelle in einem Produkt mit digitalen Elementen als Bedrohung für das Funktionieren des Binnenmarktes angesehen werden. Die Hersteller sollten behobene Sicherheitslücken der Europäischen Kommission ***offenlegen.***

| | |
|---|---|
| ***Datenbank***. | Schwachstellen-Datenbank, die gemäß der ***Richtlinie (EU) 2022/2555*** eingerichtet und von der ENISA verwaltet wird. |
| | Oder. en |

*Rechtfertigung*

*Schwachstellen, die von "White Hats" entdeckt werden, sollten nicht der Meldepflicht unterliegen.*

**Abänderung 22**

**Vorschlag für eine Verordnung**
**Erwägungsgrund 35**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (35) Die Hersteller sollten der ENISA auch alle Vorfälle melden, die sich auf die Sicherheit des Produkts mit digitalen Elementen auswirken. Ungeachtet der Meldepflicht für wesentliche und bedeutende Einrichtungen gemäß der ***Richtlinie [Richtlinie XXX/XXXX (NIS2)]*** ist es für die ENISA, die von den Mitgliedstaaten gemäß Artikel [Artikel X] der ***Richtlinie [Richtlinie XXX/XXXX (NIS2)]*** benannten einheitlichen Ansprechpartner und die Marktüberwachungsbehörden von entscheidender Bedeutung, von den Herstellern von Produkten mit digitalen Elementen Informationen zu erhalten, die es ihnen ermöglichen, die Sicherheit dieser Produkte zu bewerten. Um sicherzustellen, dass die Nutzer schnell auf Vorfälle reagieren können, die sich auf die Sicherheit ihrer Produkte mit digitalen Elementen auswirken, sollten die Hersteller ihre Nutzer auch über derartige Vorfälle und gegebenenfalls über Abhilfemaßnahmen informieren, die die Nutzer ergreifen können, um die Auswirkungen des Vorfalls abzumildern, indem sie beispielsweise einschlägige Informationen auf ihren Websites veröffentlichen oder, sofern der Hersteller | in der Lage ist, mit den Nutzern in Kontakt zu treten, und sofern dies durch die Risiken gerechtfertigt ist, die Nutzer direkt ansprechen. |

(35) Die Hersteller sollten der ENISA auch alle ***wesentlichen*** Vorfälle melden, die sich auf die Sicherheit des Produkts mit digitalen Elementen auswirken. Ungeachtet der Meldepflicht für wesentliche und bedeutende Einrichtungen gemäß der ***Richtlinie (EU) 2022/2555*** ist es für die ENISA, die von den Mitgliedstaaten gemäß Artikel [Artikel X] der ***Richtlinie (EU) 2022/2555*** benannten einheitlichen Ansprechpartner und die Marktüberwachungsbehörden von entscheidender Bedeutung, von den Herstellern von Produkten mit digitalen Elementen Informationen zu erhalten, die es ihnen ermöglichen, die Sicherheit dieser Produkte zu bewerten. Um sicherzustellen, dass die Nutzer schnell auf ***erhebliche*** Vorfälle reagieren können, die sich auf die Sicherheit ihrer Produkte mit digitalen Elementen auswirken, sollten die Hersteller ihre Nutzer auch über solche Vorfälle und gegebenenfalls über Abhilfemaßnahmen informieren, die die Nutzer ergreifen können, um die Auswirkungen des Vorfalls abzumildern, indem sie beispielsweise einschlägige Informationen auf ihren Websites veröffentlichen oder, sofern der Hersteller in der Lage ist, mit den Nutzern in Kontakt zu treten, und sofern dies durch die Risiken gerechtfertigt ist, die Nutzer direkt ansprechen.

Oder. en

**Abänderung 23**

**Vorschlag für eine Verordnung Erwägung 35 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(35a) Hersteller, andere Einrichtungen und Akteure sollten auch in der Lage sein, der ENISA auf freiwilliger Basis über andere Cybersicherheitsvorfälle, Cyberbedrohungen, Beinaheunfälle und andere Schwachstellen zu berichten.*** |

Oder. en

*Rechtfertigung*

*Im Einklang mit der Einführung eines Artikels, der eine freiwillige zusätzliche Berichterstattung ermöglicht.*

**Abänderung 24**

**Vorschlag für eine Verordnung Erwägungsgrund 37**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (37) Um die Schwachstellenanalyse zu erleichtern, sollten die Hersteller die in den Produkten enthaltenen Komponenten mit digitalen Elementen identifizieren und dokumentieren, unter anderem durch die Erstellung einer Software-Stückliste. Eine Software-Stückliste kann denjenigen, die Software herstellen, kaufen und betreiben, Informationen zur Verfügung stellen, die ihr Verständnis der Lieferkette verbessern, was mehrere Vorteile mit sich bringt, insbesondere hilft sie Herstellern und Nutzern, bekannte und neu auftretende Schwachstellen und Risiken zu verfolgen. Für Hersteller ist es besonders wichtig, sicherzustellen, dass ihre Produkte keine | von Dritten entwickelten anfälligen Komponenten enthalten. |

(37) Um die Schwachstellenanalyse zu erleichtern, sollten die Hersteller die in den Produkten enthaltenen Komponenten mit digitalen Elementen identifizieren und dokumentieren, unter anderem durch die Erstellung einer Software-Stückliste. Eine Software-Stückliste kann denjenigen, die Software herstellen, kaufen und betreiben, Informationen zur Verfügung stellen, die ihr Verständnis der Lieferkette verbessern, was mehrere Vorteile mit sich bringt, insbesondere hilft sie Herstellern und Nutzern, bekannte und neu auftretende Schwachstellen und Risiken zu verfolgen. Für die Hersteller ist es von besonderer Bedeutung, sicherzustellen, dass ihre Produkte keine von Dritten entwickelten anfälligen Komponenten enthalten. ***Die Hersteller sollten jedoch nicht verpflichtet sein, die Software-Stückliste zu veröffentlichen, da***

***Dies kann unbeabsichtigte Auswirkungen auf die Cybersicherheit ihrer Produkte mit digitalen Elementen haben.***

Oder. en

**Abänderung 25**

**Vorschlag für eine Verordnung Erwägung 41**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (41) Werden keine harmonisierten Normen angenommen oder entsprechen die harmonisierten Normen nicht in ausreichendem Maße den grundlegenden Anforderungen dieser Verordnung, sollte die Kommission die Möglichkeit haben, im Wege von Durchführungsrechtsakten gemeinsame Spezifikationen zu erlassen. ***Gründe für die Ausarbeitung solcher gemeinsamen Spezifikationen anstelle von harmonisierten Normen könnten die Ablehnung eines Normungsantrags durch eine der europäischen Normungsorganisationen,*** unangemessene Verzögerungen bei der Ausarbeitung geeigneter harmonisierter Normen ***oder die mangelnde Übereinstimmung entwickelter Normen*** mit den ***Anforderungen dieser Verordnung oder mit einem*** Ersuchen ***der Kommission sein***. Um die Bewertung der Konformität mit den in dieser Verordnung festgelegten grundlegenden Anforderungen zu erleichtern, sollte eine Konformitätsvermutung für Produkte mit digitalen Elementen gelten, die mit den von der Kommission gemäß dieser Verordnung angenommenen gemeinsamen Spezifikationen übereinstimmen, um die detaillierten technischen Spezifikationen dieser Anforderungen auszudrücken. | (41) Werden keine harmonisierten Normen angenommen oder entsprechen die harmonisierten Normen nicht in ausreichendem Maße den grundlegenden Anforderungen dieser Verordnung, sollte die Kommission die Möglichkeit haben, im Wege von Durchführungsrechtsakten gemeinsame Spezifikationen zu erlassen. ***Diese Option sollte als Ausnahmelösung betrachtet werden, wenn*** der ***Normungsprozess blockiert ist, wenn es*** bei der Ausarbeitung geeigneter harmonisierter Normen zu unangemessenen Verzögerungen kommt ***oder wenn die Ergebnisse nicht*** dem ***ursprünglichen*** Antrag entsprechen. Um die Bewertung der Konformität mit den in dieser Verordnung festgelegten grundlegenden Anforderungen zu erleichtern, sollte eine Konformitätsvermutung für Produkte mit digitalen Elementen gelten, die mit den gemeinsamen Spezifikationen übereinstimmen, die von der Kommission gemäß dieser Verordnung zum Zwecke der Formulierung detaillierter technischer Spezifikationen dieser Anforderungen angenommen wurden. |

Oder. en

*Rechtfertigung*

*Im Einklang mit den Änderungen an Artikel 19 und den GPSR wird die gemeinsame Spezifikation als letztes Mittel eingesetzt.*

**Abänderung 26**

**Vorschlag für eine Verordnung Erwägung 45**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
| --- | --- |
| (45) In der Regel sollte die Konformitätsbewertung von Produkten mit digitalen Elementen vom Hersteller in eigener Verantwortung nach dem Verfahren auf der Grundlage von Modul A des Beschlusses 768/2008/EG durchgeführt werden. Dem Hersteller sollte es freigestellt bleiben, ein strengeres Konformitätsbewertungsverfahren unter Einbeziehung eines Dritten zu wählen. Ist das Produkt als kritisches Produkt der Klasse I eingestuft, ist eine zusätzliche Sicherheit erforderlich, um die Konformität mit den in dieser Verordnung festgelegten grundlegenden Anforderungen nachzuweisen. Der Hersteller sollte harmonisierte Normen, gemeinsame Spezifikationen oder Cybersicherheitszertifizierungssysteme gemäß der Verordnung (EU) 2019/881 anwenden, die von der Kommission in einem Durchführungsrechtsakt festgelegt wurden, wenn er die Konformitätsbewertung in eigener Verantwortung durchführen möchte (Modul A). Wendet der Hersteller keine solchen harmonisierten Normen, gemeinsamen Spezifikationen oder Cybersicherheitszertifizierungssysteme an, sollte er die Konformitätsbewertung unter Einbeziehung eines Dritten durchführen. Unter Berücksichtigung des Verwaltungsaufwands für die Hersteller und der Tatsache, dass die Cybersicherheit in der Entwurfs- und Entwicklungsphase materieller und immaterieller Produkte mit digitalen Elementen eine wichtige Rolle spielt, wurden Konformitätsbewertungsverfahren auf der Grundlage der Module B+C bzw. H des | Beschlusses Nr. 768/2008/EG ausgewählt, die sich am besten eignen, um die Konformität kritischer Produkte mit digitalen Elementen auf verhältnismäßige und wirksame Weise zu bewerten. Der Hersteller, der die Drittbewertung durchführt. |

(45) In der Regel sollte die Konformitätsbewertung von Produkten mit digitalen Elementen vom Hersteller in eigener Verantwortung nach dem Verfahren auf der Grundlage von Modul A des Beschlusses 768/2008/EG durchgeführt werden. Dem Hersteller sollte es freigestellt bleiben, ein strengeres Konformitätsbewertungsverfahren unter Einbeziehung eines Dritten zu wählen. Ist das Produkt als kritisches Produkt der Klasse I eingestuft, ist eine zusätzliche Sicherheit erforderlich, um die Konformität mit den in dieser Verordnung festgelegten grundlegenden Anforderungen nachzuweisen. Der Hersteller sollte harmonisierte Normen, gemeinsame Spezifikationen oder Cybersicherheitszertifizierungssysteme gemäß der Verordnung (EU) 2019/881 anwenden, die von der Kommission in einem Durchführungsrechtsakt festgelegt wurden, wenn er die Konformitätsbewertung in eigener Verantwortung durchführen möchte (Modul A)***, vorausgesetzt, dass diese harmonisierten Normen, gemeinsamen Spezifikationen oder Cybersicherheitszertifizierungssysteme bereits seit einem Mindestzeitraum in Kraft sind, der es den Herstellern ermöglicht, sie zu übernehmen***. Wendet der Hersteller solche harmonisierten Normen, gemeinsamen Spezifikationen oder Cybersicherheitszertifizierungssysteme nicht an, sollte er sich einer Konformitätsbewertung unter Einbeziehung einer dritten Partei unterziehen. In Anbetracht des Verwaltungsaufwands für die Hersteller und der Tatsache, dass die Cybersicherheit in der Entwurfs- und Entwicklungsphase materieller und immaterieller Produkte mit digitalen Elementen eine wichtige Rolle spielt, wurden Konformitätsbewertungsverfahren auf der Grundlage der Module B+C bzw. Modul H des Beschlusses 768/2008/EG

| | |
|---|---|
| Konformitätsbewertung das Verfahren wählen, das sich am besten für seinen Entwurfs- und Produktionsprozess eignet. Angesichts des noch größeren Cybersicherheitsrisikos, das mit der Verwendung von als kritische Produkte der Klasse II eingestuften Produkten verbunden ist, sollte die Konformitätsbewertung immer von einer dritten Partei durchgeführt werden. | wurde als am besten geeignet ausgewählt, um die Konformität kritischer Produkte mit digitalen Elementen auf verhältnismäßige und wirksame Weise zu bewerten. Der Hersteller, der die Konformitätsbewertung durch einen Dritten durchführt, kann das Verfahren wählen, das seinem Entwurfs- und Produktionsprozess am besten entspricht. In Anbetracht des noch größeren Risikos für die Cybersicherheit, das mit der Verwendung von als kritische Produkte der Klasse II eingestuften Produkten verbunden ist, sollte die Konformitätsbewertung stets von einer dritten Partei durchgeführt werden. |
| | Oder. en |

**Abänderung 27**

**Vorschlag für eine Verordnung Erwägung 46 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(46a) Diese Verordnung erlegt den Wirtschaftsakteuren komplexe Verpflichtungen auf, insbesondere den Herstellern von Softwareprodukten und den Kleinst-, kleinen und mittleren Unternehmen. Die Kommission sollte daher Leitlinien in Form eines Handbuchs für Wirtschaftsteilnehmer herausgeben, in dem die praktischen Auswirkungen dieser Verordnung ausführlich und klar erläutert werden. Diese Leitlinien sollten unter anderem eine Erläuterung des Begriffs der Datenfernverarbeitung, eine Beschreibung der Methodik zur Bestimmung kritischer Produkte mit digitalen Elementen und eine Erläuterung der Wechselwirkung zwischen dieser Verordnung und anderem Unionsrecht enthalten.*** |

Oder. en

**Abänderung 28**

**Vorschlag für eine**
**Verordnung**
**Erwägungsgrund 53**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (53) Im Interesse der Wettbewerbsfähigkeit ist es von entscheidender Bedeutung, dass die notifizierten Stellen die Konformitätsbewertungsverfahren anwenden, ohne ***die*** Wirtschaftsakteure unnötig zu belasten. Aus demselben Grund und um die Gleichbehandlung der Wirtschaftsakteure zu gewährleisten, muss die einheitliche technische Anwendung der Konformitätsbewertungsverfahren sichergestellt werden. Dies sollte am besten durch eine angemessene Koordinierung und Zusammenarbeit zwischen den notifizierten Stellen erreicht werden. | (53) Im Interesse der Wettbewerbsfähigkeit ist es von entscheidender Bedeutung, dass die notifizierten Stellen die Konformitätsbewertungsverfahren anwenden, ohne ***die*** Wirtschaftsakteure unnötig zu belasten***. Die Kommission und die Mitgliedstaaten sollten daher sicherstellen, dass in der Union ausreichend qualifizierte Fachkräfte zur Verfügung stehen, damit die notifizierten Konformitätsbewertungsstellen ihre Tätigkeiten schnell und effizient durchführen können und Engpässe auf ein Mindestmaß beschränkt werden***. Aus demselben Grund und um die Gleichbehandlung der Wirtschaftsakteure zu gewährleisten, muss die Kohärenz bei der technischen Anwendung der Konformitätsbewertungsverfahren sichergestellt werden. Dies sollte am besten durch eine angemessene Koordinierung und Zusammenarbeit zwischen den benannten Stellen erreicht werden. |

Oder. en

**Abänderung 29**

**Vorschlag für eine**
**Verordnung**
**Erwägungsgrund 61**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (61) Gleichzeitige koordinierte Kontrollmaßnahmen ("Sweeps") sind spezifische Durchsetzungsmaßnahmen der Marktaufsichtsbehörden, die die | Produktsicherheit weiter verbessern können. Sweeps sollten insbesondere dann durchgeführt werden, wenn Markttrends, Verbraucherbeschwerden oder andere Hinweise |

darauf hindeuten, dass bestimmte Produktkategorien häufig mit Cybersicherheitsrisiken behaftet sind. Die ENISA sollte der Kommission Vorschläge für Produktkategorien vorlegen, für die Sweeps organisiert werden könnten.

(61) Gleichzeitige koordinierte Kontrollmaßnahmen ("Sweeps") sind spezifische Durchsetzungsmaßnahmen der Marktaufsichtsbehörden, die die Produktsicherheit weiter verbessern können. Sweeps sollten insbesondere dann durchgeführt werden, wenn Markttrends, Verbraucherbeschwerden oder andere Hinweise darauf hindeuten, dass bestimmte Produktkategorien häufig mit Cybersicherheitsrisiken behaftet sind. Die ENISA sollte der Kommission Vorschläge für Produktkategorien vorlegen, für die Sweeps organisiert werden könnten.

| | |
|---|---|
| Marktaufsichtsbehörden, u. a. auf der Grundlage der bei ihr eingehenden Meldungen über Produktschwachstellen und -vorfälle. | Marktaufsichtsbehörden, unter anderem auf der Grundlage der bei ihr eingehenden Meldungen über Produktschwachstellen und Zwischenfälle. ***Besonderes Augenmerk sollte auf Produkte mit digitalen Elementen gelegt werden, die von Herstellern auf den Markt gebracht werden und ein Sicherheitsrisiko für die Union darstellen könnten, auch im Hinblick auf den geopolitischen Kontext.*** |

Oder. en

**Abänderung 30**

**Vorschlag für eine Verordnung Erwägung 61 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(61a) Bedenken hinsichtlich der Wirtschaftsakteure, die ein Sicherheitsrisiko für die Union darstellen könnten, sollten jedoch erfordern, dass geeignete Schutzmaßnahmen ergriffen werden und eine gründliche Prüfung ihrer Produkte mit digitalen Elementen gewährleistet wird. Daher sollte die ENISA eine koordinierende Rolle übernehmen, um sicherzustellen, dass die Marktüberwachungsbehörden solche Produkte mit digitalen Elementen regelmäßig überprüfen, insbesondere um potenzielle eingebaute Hintertüren oder andere ausnutzbare Schwachstellen zu ermitteln.*** |

Oder. en

**Abänderung 31**

**Vorschlag für eine Verordnung Erwägung 62**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
| --- | --- |
| (62) Um sicherzustellen, dass der Rechtsrahmen erforderlichenfalls angepasst werden kann, wird die Befugnis zum Erlass von Rechtsakten in | (62) Um sicherzustellen, dass der Rechtsrahmen erforderlichenfalls angepasst werden kann, wird die Befugnis zum Erlass von Rechtsakten in |

Die Befugnis zum Erlass von Rechtsakten gemäß Artikel 290 des Vertrags sollte der Kommission übertragen werden, um die Liste der kritischen Produkte in Anhang III zu aktualisieren und die Begriffsbestimmungen für diese Produktkategorien festzulegen. Der Kommission sollte die Befugnis übertragen werden, gemäß dem genannten Artikel Rechtsakte zu erlassen, um Produkte mit digitalen Elementen zu ermitteln, die unter andere Unionsvorschriften fallen, mit denen das gleiche Schutzniveau wie mit dieser Verordnung erreicht wird, wobei anzugeben ist, ob eine Einschränkung oder ein Ausschluss vom Anwendungsbereich dieser Verordnung erforderlich ist, sowie gegebenenfalls der Umfang dieser Einschränkung. Die Befugnis zum Erlass von Rechtsakten gemäß dem genannten Artikel sollte der Kommission auch in Bezug auf die mögliche Verpflichtung zur Zertifizierung bestimmter hochkritischer Produkte mit digitalen Elementen auf der Grundlage der in dieser Verordnung festgelegten Kritikalitätskriterien sowie zur Festlegung des Mindestinhalts der EU-Konformitätserklärung und zur Ergänzung der in die technischen Unterlagen aufzunehmenden Elemente übertragen werden. Es ist von besonderer Bedeutung, dass die Kommission bei ihren vorbereitenden Arbeiten angemessene Konsultationen, auch auf Expertenebene, durchführt und dass diese Konsultationen im Einklang mit den Grundsätzen der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung[33] durchgeführt werden. Um insbesondere eine gleichberechtigte Beteiligung an der Ausarbeitung delegierter Rechtsakte zu gewährleisten, erhalten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten, und ihre Sachverständigen haben systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission, die mit der Ausarbeitung der delegierten Rechtsakte befasst sind.

Die Befugnis zum Erlass von Rechtsakten gemäß Artikel 290 des Vertrags sollte der Kommission übertragen werden, um die Liste der kritischen Produkte in Anhang III zu aktualisieren und die Begriffsbestimmungen für diese Produktkategorien festzulegen. Der Kommission sollte die Befugnis übertragen werden, gemäß dem genannten Artikel Rechtsakte zu erlassen, um Produkte mit digitalen Elementen zu ermitteln, die unter andere Unionsvorschriften fallen, mit denen das gleiche Schutzniveau wie mit dieser Verordnung erreicht wird, wobei anzugeben ist, ob eine Einschränkung oder ein Ausschluss vom Anwendungsbereich dieser Verordnung erforderlich ist, sowie gegebenenfalls der Umfang dieser Einschränkung. Die Befugnis zum Erlass von Rechtsakten gemäß dem genannten Artikel sollte der Kommission auch in Bezug auf die mögliche Verpflichtung zur Zertifizierung bestimmter hochkritischer Produkte mit digitalen Elementen auf der Grundlage der in dieser Verordnung festgelegten Kritikalitätskriterien sowie zur Festlegung des Mindestinhalts der EU-Konformitätserklärung und zur Ergänzung der in die technischen Unterlagen aufzunehmenden Elemente übertragen werden. ***Die Kommission sollte auch das Format und die Elemente der Software-Stückliste festlegen und die Art der Informationen, das Format und das Verfahren für die Meldungen über aktiv ausgenutzte Schwachstellen und bedeutende Vorfälle, die der ENISA von den Herstellern vorgelegt werden, näher bestimmen. Erforderlichenfalls sollte der Kommission die Befugnis übertragen werden, delegierte Rechtsakte zum Erlass gemeinsamer Spezifikationen in Bezug auf die in Anhang I aufgeführten grundlegenden Anforderungen zu erlassen.*** Es ist von besonderer Bedeutung, dass die Kommission bei ihren vorbereitenden Arbeiten angemessene Konsultationen durchführt, auch auf Expertenebene ***und insbesondere mit der***

***Sachverständigengruppe***, und dass diese Konsultationen im Einklang mit den in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung[33] festgelegten Grundsätzen durchgeführt werden. Um insbesondere eine gleichberechtigte Beteiligung an der Ausarbeitung delegierter Rechtsakte zu gewährleisten, erhalten das Europäische Parlament und der Rat alle

| | |
|---|---|
| | Ihre Experten haben systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission, die sich mit der Ausarbeitung delegierter Rechtsakte befassen, und können die Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten einsehen. |
| [33] ABl. L 123 vom 12.5.2016, S. 1. | [33] ABl. L 123 vom 12.5.2016, S. 1. |

Oder. en

*Rechtfertigung*

*Angleichung an neue delegierte Rechtsakte, einschließlich der Fälle, in denen der Kommissionsvorschlag Durchführungsrechtsakte vorsieht.*

**Abänderung 32**

**Vorschlag für eine Verordnung**
**Erwägungsgrund 63**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (63) Um einheitliche Bedingungen für die Durchführung dieser Verordnung zu gewährleisten, sollten der Kommission Durchführungsbefugnisse übertragen werden, um: ***das Format und die Elemente der Software-Stückliste zu spezifizieren, die Art der Informationen, das Format und das Verfahren der Meldungen über aktiv ausgenutzte Schwachstellen und Vorfälle, die der ENISA von den Herstellern übermittelt werden, näher zu*** spezifizieren, die gemäß der Verordnung (EU) 2019/881 angenommenen europäischen Cybersicherheits-Zertifizierungssysteme zu spezifizieren, die für den Nachweis der Konformität mit den in Anhang I dieser Verordnung aufgeführten grundlegenden Anforderungen oder Teilen davon verwendet werden können***, gemeinsame Spezifikationen für die in Anhang I aufgeführten grundlegenden*** | ***Anforderungen zu verabschieden***, technische Spezifikationen für Piktogramme oder andere Zeichen im Zusammenhang mit der Sicherheit von Produkten mit digitalen Elementen sowie Mechanismen zur Förderung ihrer Verwendung festzulegen und unter außergewöhnlichen Umständen über korrigierende oder restriktive Maßnahmen auf Unionsebene zu entscheiden |

(63) Um einheitliche Bedingungen für die Durchführung dieser Verordnung zu gewährleisten, sollten der Kommission Durchführungsbefugnisse übertragen werden, um: die gemäß der Verordnung (EU) 2019/881 angenommenen europäischen Zertifizierungssysteme für Cybersicherheit zu spezifizieren, die für den Nachweis der Konformität mit den in Anhang I dieser Verordnung aufgeführten grundlegenden Anforderungen oder Teilen davon verwendet werden können, technische Spezifikationen für Piktogramme oder andere Zeichen im Zusammenhang mit der Sicherheit von Produkten mit digitalen Elementen sowie Mechanismen zur Förderung ihrer Verwendung festzulegen, über korrigierende oder restriktive Maßnahmen auf Unionsebene zu entscheiden, wenn außergewöhnliche Umstände vorliegen, die ein sofortiges Eingreifen zur Wahrung des reibungslosen Funktionierens des Binnenmarkts rechtfertigen. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des [Rates34] ausgeübt werden.

die ein sofortiges Eingreifen rechtfertigen, um das reibungslose Funktionieren des Binnenmarkts zu gewährleisten. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates[34] ausgeübt werden.

[34] Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

[34] Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011),
p. 13).

Oder. en

*Rechtfertigung*

*Delegierte Rechtsakte sind für diese Elemente besser geeignet.*

**Abänderung 33**

**Vorschlag für eine**
**Verordnung**
**Erwägungsgrund 65**

*Von der Kommission vorgeschlagener Text*

*g*

(65) Um eine wirksame Durchsetzung der in dieser Verordnung festgelegten Verpflichtungen zu gewährleisten, sollte jede Marktüberwachungsbehörde befugt sein, Verwaltungsgeldbußen zu verhängen oder deren Verhängung zu beantragen. Es sollten daher Höchstbeträge für Verwaltungsgeldbußen festgelegt werden , die in den nationalen Rechtsvorschriften für die Nichteinhaltung der in dieser Verordnung festgelegten Verpflichtungen vorzusehen sind. Bei der

*Abänderun*

Entscheidung über die Höhe der Geldbuße in jedem Einzelfall sollten alle relevanten Umstände der jeweiligen Situation und zumindest die in dieser Verordnung ausdrücklich festgelegten Umstände berücksichtigt werden, einschließlich der Frage, ob bereits Geldbußen verhängt wurden

(65) Um eine wirksame Durchsetzung der in dieser Verordnung festgelegten Verpflichtungen zu gewährleisten, sollte jede Marktüberwachungsbehörde befugt sein, Verwaltungsgeldbußen zu verhängen oder deren Verhängung zu beantragen. Es sollten daher Höchstbeträge für Verwaltungsgeldbußen festgelegt werden, die in den nationalen Rechtsvorschriften für die Nichteinhaltung der in dieser Verordnung festgelegten Verpflichtungen vorzusehen sind. Bei der Entscheidung über die Höhe der Geldbuße in jedem Einzelfall sollten alle relevanten Umstände der jeweiligen Situation und zumindest die in dieser Verordnung ausdrücklich festgelegten Umstände berücksichtigt werden, einschließlich der Frage, ob bereits Geldbußen verhängt wurden

| | |
|---|---|
| die von anderen Marktüberwachungsbehörden gegen denselben Betreiber wegen ähnlicher Verstöße verhängt wurden. Solche Umstände können entweder erschwerend sein, wenn der Verstoß desselben Wirtschaftsakteurs im Hoheitsgebiet anderer Mitgliedstaaten als demjenigen, in dem bereits eine Verwaltungsgeldbuße verhängt wurde, andauert, oder mildernd, indem sichergestellt wird, dass bei jeder weiteren Verwaltungsgeldbuße, die eine andere Marktüberwachungsbehörde für denselben Wirtschaftsakteur oder dieselbe Art von Verstoß in Erwägung zieht, bereits eine in anderen Mitgliedstaaten verhängte Sanktion und deren Höhe zusammen mit anderen relevanten spezifischen Umständen berücksichtigt werden sollten. In allen diesen Fällen sollte die kumulative Geldbuße, die von den Marktüberwachungsbehörden mehrerer Mitgliedstaaten gegen denselben Wirtschaftsakteur für dieselbe Art von Verstoß verhängt werden könnte, die Einhaltung des Grundsatzes der Verhältnismäßigkeit gewährleisten. | die von anderen Marktüberwachungsbehörden wegen ähnlicher Verstöße gegen denselben Wirtschaftsakteur verhängt wurden, sowie die Tatsache***, ob es sich bei dem Wirtschaftsakteur um ein Kleinstunternehmen, ein kleines oder ein mittleres Unternehmen handelt***. Diese Umstände können entweder erschwerend wirken, wenn der Verstoß desselben Wirtschaftsakteurs im Hoheitsgebiet anderer Mitgliedstaaten als demjenigen, in dem bereits eine Geldbuße verhängt wurde, fortbesteht, oder mildernd, indem sie sicherstellen, dass bei jeder weiteren von einer anderen Marktüberwachungsbehörde für denselben Wirtschaftsakteur oder dieselbe Art von Verstoß in Betracht gezogenen Geldbuße neben anderen relevanten spezifischen Umständen bereits eine in anderen Mitgliedstaaten verhängte Sanktion und deren Höhe berücksichtigt werden. In allen diesen Fällen sollte die kumulative Geldbuße, die von den Marktüberwachungsbehörden mehrerer Mitgliedstaaten gegen denselben Wirtschaftsakteur für dieselbe Art von Verstoß verhängt werden könnte, die Einhaltung des Grundsatzes der Verhältnismäßigkeit gewährleisten. |

Oder. en

**Abänderung 34**

**Vorschlag für eine Verordnung Erwägung 66 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(66a) Die Einnahmen aus der Verhängung von Sanktionen gemäß dieser Verordnung sollten zur Anhebung des Niveaus der Cybersicherheit in der Union verwendet werden, indem Programme gefördert werden, die*** |

***darauf abzielen, den Ausbau und die optimale Nutzung der europäischen Kenntnisse, Kapazitäten und Fähigkeiten im Bereich der Cybersicherheit sowie den Austausch und die durchgängige Anwendung bewährter Verfahren zu unterstützen. Zu diesem Zweck sollten diese Einnahmen dem spezifischen Ziel "Cybersicherheit und Vertrauen" des Programms "Digitales Europa" zugewiesen werden***

| | |
|---|---|
| | ***Programm gemäß Artikel 6 der Verordnung (EU) 2021/694. Diese Mittel sollten als Aufstockung dieser Haushaltslinie betrachtet werden und sollten den Beitrag aus dem Haushalt der Union nicht verringern.*** |

Oder. en

**Abänderung 35**

**Vorschlag für eine**
**Verordnung**
**Erwägungsgrund 68**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (68) Die Kommission sollte diese Verordnung in regelmäßigen Abständen in Konsultation mit den interessierten Parteien überprüfen, um insbesondere festzustellen, ob sie angesichts veränderter gesellschaftlicher, politischer, technologischer oder marktbezogener Bedingungen geändert werden muss. | (68) Die Kommission sollte diese Verordnung in regelmäßigen Abständen in Absprache mit ***der Sachverständigengruppe und anderen*** interessierten Parteien überprüfen, um insbesondere festzustellen, ob sie angesichts veränderter gesellschaftlicher, politischer, technologischer oder marktbezogener Bedingungen geändert werden muss. |

Oder. en

**Abänderung 36**

**Vorschlag für eine**
**Verordnung**
**Erwägungsgrund 69**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (69) Den Wirtschaftsakteuren sollte ausreichend Zeit eingeräumt werden, um sich an die Anforderungen dieser Verordnung anzupassen. Diese Verordnung sollte [***24*** Monate] ab ihrem Inkrafttreten gelten, mit Ausnahme der Meldepflichten für aktiv ausgenutzte Schwachstellen und Vorfälle, die [***12*** | Monate] ab dem Inkrafttreten dieser Verordnung gelten sollten. |

(69) Den Wirtschaftsakteuren sollte ausreichend Zeit eingeräumt werden, um sich an die Anforderungen dieser Verordnung anzupassen. Diese Verordnung sollte [***40*** Monate] ab ihrem Inkrafttreten gelten, mit Ausnahme der Meldepflichten für aktiv ausgenutzte Schwachstellen und Zwischenfälle, die [***20*** Monate] ab dem Inkrafttreten dieser Verordnung gelten sollten.

Oder. en

*Rechtfertigung*

*Angesichts des horizontalen Charakters, des breiten Anwendungsbereichs und der Komplexität dieser Verordnung sollte den Wirtschaftsbeteiligten ausreichend Zeit zur Anpassung an diese Verordnung eingeräumt werden.*

**Abänderung 37**

**Vorschlag für eine**
**Verordnung Erwägung**
**69 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(69a) Um Kleinstunternehmen sowie kleine und mittlere Unternehmen zu unterstützen und ihnen zu helfen, die zusätzlichen Kosten zu bewältigen, die sich aus dieser Verordnung ergeben können, sollte die Kommission eine angemessene finanzielle und technische Unterstützung bereitstellen, die es diesen Unternehmen ermöglicht, zum Wachstum der europäischen Wirtschaft beizutragen und das Niveau ihrer Cybersicherheit zu erhöhen.*** |

Oder. en

**Abänderung 38**

**Vorschlag für eine**
**Verordnung Erwägung**
**71 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(71a) Die Kommission sollte den dieser Verordnung beigefügten Finanzbogen dahingehend ändern, dass die ENISA mit 8,5 zusätzlichen Vollzeitstellen und entsprechenden zusätzlichen Mitteln ausgestattet wird, um ihre in dieser Verordnung vorgesehenen zusätzlichen Aufgaben zu erfüllen.*** |

Oder. en

**Abänderung 39**

**Vorschlag für eine**
**Verordnung Artikel 2 -**
**Absatz 1**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 1. Diese Verordnung gilt für Produkte mit digitalen Elementen***, deren bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine*** direkte oder indirekte ***logische oder physische*** Datenverbindung zu einem Gerät oder Netz ***umfasst***. | 1. Diese Verordnung gilt für Produkte mit digitalen Elementen***, die*** eine direkte oder indirekte Datenverbindung zu einem Gerät oder Netz ***haben können***. |

Oder. en

*Rechtfertigung*

*Es ist notwendig, den Anwendungsbereich zu vereinfachen, um ihn für Bürger und Unternehmen gleichermaßen verständlicher zu machen.*

**Abänderung 40**

**Vorschlag für eine**

**Verordnung**
**Artikel 2 - Absatz 4 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(4a) Diese Verordnung gilt nicht für Bauteile, die ausschließlich als Ersatzteile für andere Produkte mit digitalen Elementen hergestellt werden, die vor dem ... [40 Monate nach Inkrafttreten dieser Verordnung] in Verkehr gebracht wurden. [40 Monate nach dem Inkrafttreten dieser Verordnung] in Verkehr gebracht wurden.*** |

Oder. en

*Rechtfertigung*

*Um sicherzustellen, dass Produkte, die bereits vor dem Inkrafttreten dieser Verordnung auf dem Markt waren, repariert und ihre Lebensdauer verlängert werden können, ist es*

*notwendig, eine Ausnahmeregelung für Ersatzteile vorzusehen.*

**Abänderung 41**

**Vorschlag für eine Verordnung**
**Artikel 3 - Absatz 1 - Nummer 2**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (2) "Datenfernverarbeitung" ist jede Datenverarbeitung aus der Ferne, für die die Software vom Hersteller oder unter der Verantwortung des Herstellers konzipiert und entwickelt wurde und deren Fehlen das Produkt mit digitalen Elementen daran hindern würde, eine seiner Funktionen zu erfüllen; | (2) "Datenfernverarbeitung" ist jede Datenverarbeitung aus der Ferne, für die die Software vom Hersteller oder unter der Verantwortung des Herstellers konzipiert und entwickelt wurde und deren Fehlen das Produkt mit digitalen Elementen daran hindern würde, eine seiner Kernfunktionen zu erfüllen; |

Oder. en

*Rechtfertigung*

*Datenfernverarbeitungslösungen sollten abgedeckt werden, wenn sie für das Funktionieren des Produkts mit digitalen Elementen von zentraler Bedeutung sind.*

**Abänderung 42**

**Vorschlag für eine**

**Verordnung**
**Artikel 3 - Absatz 1 - Nummer 4 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(4a) "Cybersicherheit" ist Cybersicherheit im Sinne von Artikel 2 Nummer 1 der Verordnung (EU) 2019/881;*** |

Oder. en

*Rechtfertigung*

*Verweis auf die im Cybersicherheitsgesetz enthaltene Definition von Cybersicherheit.*

**Abänderung 43**

**Vorschlag für eine**

**Verordnung**
**Artikel 3 - Absatz 1 - Nummer 21 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(21a) "Kleinstunternehmen sowie kleine und mittlere Unternehmen" sind Kleinstunternehmen sowie kleine und mittlere Unternehmen im Sinne der Empfehlung [2003/361/EG1a] der Kommission;*** |
| | ***[1a] Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (Bekannt gegeben unter Aktenzeichen K(2003) 1422) (ABl. L 124 vom 20.5.2003, S. 1). 36).*** |

Oder. en

**Abänderung 44**

**Vorschlag für eine**

**Verordnung**
**Artikel 3 - Absatz 1 - Nummer 39 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(39a) "Störung": eine Störung gemäß der Definition in Artikel 6 Nummer 6 der Richtlinie (EU) 2022/2555;*** |

Oder. en

**Abänderung 45**

**Vorschlag für eine**

**Verordnung**
**Artikel 3 - Absatz 1 - Nummer 39 b (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(39b) "Beinaheunfall": ein Beinaheunfall gemäß der Definition in*** |

***Artikel 6 Nummer 5 der Richtlinie (EU) 2022/2555;***

Oder. en

*Rechtfertigung*

*Die in der NIS 2 enthaltene Definition des Begriffs "Beinaheunfall" wird für die freiwillige Meldung in dem neu geschaffenen Artikel 11a verwendet.*

**Abänderung 46**

**Vorschlag für eine**

**Verordnung**
**Artikel 3 - Absatz 1 - Nummer 39 c (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(39c) "Cyber-Bedrohung" ist eine Cyber-Bedrohung im Sinne von Artikel 2 Nummer 8 der Verordnung (EU) 2019/881;*** |

Oder. en

*Rechtfertigung*

*Die im Cybersicherheitsgesetz enthaltene Definition der Cyber-Bedrohung wird für die freiwillige Meldung im neu geschaffenen Artikel 11a verwendet.*

**Abänderung 47**

**Vorschlag für eine**

**Verordnung**
**Artikel 6 - Absatz 2 - einleitender Teil**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 2. Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte gemäß Artikel 50 zu erlassen, um Anhang III zu ändern, indem sie in die Liste der Kategorien kritischer Produkte mit digitalen Bestandteilen eine neue Kategorie aufnimmt oder eine bestehende Kategorie aus dieser Liste streicht. Bei der Beurteilung der Notwendigkeit einer Änderung der Liste in Anhang III berücksichtigt die Kommission das Ausmaß des Cybersicherheitsrisikos im | Zusammenhang mit der Kategorie von Produkten mit digitalen Bestandteilen. Bei der Bestimmung des Ausmaßes des Cybersicherheitsrisikos sind eines oder mehrere der folgenden Kriterien zu berücksichtigen: |

2. ***Nach ... [zwei Jahre nach Inkrafttreten dieser Verordnung] und danach höchstens alle zwei Jahre wird der Kommission die*** Befugnis übertragen, delegierte Rechtsakte gemäß Artikel 50 zu erlassen, um Anhang III zu ändern, indem sie in die Liste der Kategorien kritischer Produkte mit digitalen Bestandteilen eine neue Kategorie aufnimmt oder eine bestehende Kategorie aus dieser Liste streicht. Bei der Beurteilung der Notwendigkeit einer Änderung der Liste in Anhang III berücksichtigt die Kommission das Ausmaß des Cybersicherheitsrisikos im Zusammenhang mit der Kategorie von Produkten mit digitalen Bestandteilen. Bei der Bestimmung des Ausmaßes des Cybersicherheitsrisikos sind eines oder mehrere der folgenden Kriterien zu berücksichtigen

Konto:

Oder. en

*Rechtfertigung*

*Im Interesse der Rechtsklarheit und der Vorhersehbarkeit muss sichergestellt werden, dass die Liste der kritischen Produkte nur einmal alle zwei Jahre geändert werden kann.*

**Abänderung 48**

**Vorschlag für eine**
**Verordnung Artikel 6 -**
**Absatz 3**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 3. Der Kommission wird die Befugnis übertragen, gemäß Artikel 50 einen delegierten Rechtsakt zur Ergänzung dieser Verordnung zu erlassen, in dem die Begriffsbestimmungen für die Produktkategorien der Klassen I und II gemäß Anhang III festgelegt werden. Der delegierte Rechtsakt ist [innerhalb von ***12*** Monaten nach Inkrafttreten dieser Verordnung] zu erlassen. | 3. Der Kommission wird die Befugnis übertragen, gemäß Artikel 50 einen delegierten Rechtsakt zur Ergänzung dieser Verordnung zu erlassen, in dem die Begriffsbestimmungen für die Produktkategorien der Klassen I und II gemäß Anhang III festgelegt werden. Der delegierte Rechtsakt ist [innerhalb von ***6*** Monaten nach Inkrafttreten dieser Verordnung] zu erlassen. |

Oder. en

*Rechtfertigung*

*Eine rasche Festlegung der Produktkategorien ist unerlässlich, um den Unternehmen genügend Zeit für die Anpassung an diese Verordnung zu geben.*

**Abänderung 49**

**Vorschlag für eine**

**Verordnung**
**Artikel 6 - Absatz 4 - Unterabsatz 1 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(3) Wird eine neue Kategorie kritischer Produkte mit digitalen Elementen mittels eines delegierten Rechtsakts gemäß*** |

***Absatz 2 des vorliegenden Artikels in die Liste in Anhang III aufgenommen, so wird sie innerhalb von 12 Monaten nach dem Inkrafttreten des Artikels 24 Absätze 2 und 3 den einschlägigen Konformitätsbewertungsverfahren unterzogen.***

***das Datum des Erlasses des entsprechenden delegierten Rechtsakts.***

Oder. en

*Rechtfertigung*

*Für die Hersteller kritischer Produkte, die bereits in Anhang III aufgeführt sind, gilt eine Übergangsfrist zwischen dem Inkrafttreten und der Umsetzung dieser Verordnung. Daher sollte auch für kritische Produkte, die nach dem Inkrafttreten dieser Verordnung neu in die Liste aufgenommen werden, eine Übergangsfrist vorgesehen werden.*

**Abänderung 50**

**Vorschlag für eine**

**Verordnung**
**Artikel 6 - Absatz 5 - einleitender Teil**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (5) Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte gemäß Artikel 50 zu erlassen, um diese Verordnung durch die Festlegung von Kategorien hochkritischer Produkte mit digitalen Elementen zu ergänzen, für die die Hersteller ein europäisches Cybersicherheitszertifikat im Rahmen eines europäischen Cybersicherheitszertifizierungssystems gemäß der Verordnung (EU) 2019/881 erhalten müssen, um die Konformität mit den in Anhang I aufgeführten grundlegenden Anforderungen oder Teilen davon nachzuweisen. Bei der Festlegung solcher Kategorien hochkritischer Produkte mit digitalen Bestandteilen berücksichtigt die Kommission das Ausmaß des Cybersicherheitsrisikos, das mit der Kategorie von Produkten mit digitalen Bestandteilen verbunden ist, im Hinblick auf eines oder mehrere der in Absatz 2 aufgeführten Kriterien sowie im Hinblick auf die Bewertung, ob diese Kategorie von Produkten ist: | (5) Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte gemäß Artikel 50 zu erlassen, um diese Verordnung durch die Festlegung von Kategorien hochkritischer Produkte mit digitalen Elementen zu ergänzen, für die die Hersteller ein europäisches Cybersicherheitszertifikat im Rahmen eines europäischen Cybersicherheitszertifizierungssystems gemäß der Verordnung (EU) 2019/881 erhalten müssen, um die Konformität mit den in Anhang I aufgeführten grundlegenden Anforderungen oder Teilen davon nachzuweisen. ***Die Verpflichtung, ein europäisches Cybersicherheitszertifikat zu erlangen, gilt 12 Monate nach Erlass des einschlägigen delegierten Rechtsakts.*** Bei der Festlegung solcher Kategorien hochkritischer Produkte mit digitalen Bestandteilen berücksichtigt die Kommission das Ausmaß des Cybersicherheitsrisikos, das mit der Kategorie von Produkten mit digitalen Bestandteilen verbunden ist, im Hinblick auf eines oder mehrere der in Absatz 2 |

aufgeführten Kriterien sowie im Hinblick auf die Bewertung, ob diese Kategorie von Produkten:

Oder. en

*Rechtfertigung*

*Für Produkte, für die ein europäisches Cybersicherheitszertifikat erforderlich ist, sollte eine Übergangsfrist von 12 Monaten gelten.*

**Abänderung 51**

**Vorschlag für eine**

**Verordnung**
**Artikel 6 - Absatz 5 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(5a) Der Kommission wird die Befugnis übertragen, die in Absatz 5 dieses Artikels genannten delegierten Rechtsakte frühestens 12 Monate nach der Annahme des einschlägigen europäischen Cybersicherheitszertifizierungssystems gemäß der Verordnung (EU) 2019/881 zu erlassen.*** |

Oder. en

*Rechtfertigung*

*Für neue europäische Cybersicherheitszertifizierungssysteme sollte eine Mindestlaufzeit vorgesehen werden, um ihre ordnungsgemäße Funktionsweise zu gewährleisten und den Unternehmen ausreichend Zeit für ihre Einführung zu geben.*

**Abänderung 52**

**Vorschlag für eine**

**Verordnung**
**Artikel 6 - Absatz 5 b (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(5b) Vor dem Erlass der in den Absätzen 2, 4 und 5 des vorliegenden Artikels genannten delegierten Rechtsakte konsultiert die Kommission die in [Artikel 6a] genannte Expertengruppe.*** |

Oder. en

*Rechtfertigung*

*Die Konsultation der Interessengruppen ist für das Funktionieren dieser Verordnung von wesentlicher Bedeutung. Die*

*Die Kommission sollte die neu geschaffene Expertengruppe für Cyber-Resilienz eingehend konsultieren.*

**Abänderung 53**

**Vorschlag für eine Verordnung Artikel 6 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***Artikel 6a*** |
| | ***Expertengruppe zur Widerstandsfähigkeit im Internet*** |
| | ***1. Bis zum ... [6 Monate nach Inkrafttreten dieser Verordnung] setzt die Kommission eine Sachverständigengruppe für die Widerstandsfähigkeit gegenüber Cyberangriffen (die "Sachverständigengruppe") ein. Die Zusammensetzung der Expertengruppe soll geschlechtsspezifisch und geografisch ausgewogen sein und umfasst Folgendes:*** |
| | ***(a) Vertreter jedes der folgenden Länder:*** |
| | ***(i) der Agentur der Europäischen Union für Cybersicherheit;*** |
| | ***(ii) der Europäische Datenschutzausschuss;*** |
| | ***(iii) Europol;*** |
| | ***(iv) die Europäische Verteidigungsagentur;*** |
| | ***(b) Sachverständige, die die einschlägigen privaten Interessengruppen vertreten, wobei eine angemessene Vertretung von Kleinst-, Klein- und mittleren Unternehmen sichergestellt wird;*** |
| | ***(c) Experten, die die Zivilgesellschaft, einschließlich Verbraucherorganisationen, vertreten;*** |
| | ***(d) ad personam ernannte Sachverständige, die nachweislich über Kenntnisse und Erfahrungen in den von dieser Verordnung erfassten Bereichen verfügen;*** |

***(e) Experten aus dem akademischen Bereich, einschließlich Universitäten, Forschungsinstituten und anderen wissenschaftlichen Organisationen, einschließlich Personen mit weltweitem Fachwissen.***

***2. Die Expertengruppe berät die***

***Kommission in Bezug auf die folgenden Punkte:***

***(a) die in Anhang III enthaltene Liste kritischer Produkte mit digitalen Elementen sowie die etwaige Notwendigkeit einer Aktualisierung dieser Liste;***

***(b) die Umsetzung der europäischen Cybersicherheitszertifizierungssysteme gemäß der Verordnung (EU) 2019/881 und die Möglichkeit, diese für hochkritische Produkte mit digitalen Elementen verbindlich vorzuschreiben;***

***(c) die Elemente der Verordnung, die in den Leitlinien nach Artikel 17a behandelt werden sollen;***

***(d) die Verfügbarkeit und die Qualität der europäischen und internationalen Normen sowie die Möglichkeit, diese durch gemeinsame technische Spezifikationen zu ergänzen oder zu ersetzen;***

***(e) die Verfügbarkeit von qualifizierten Fachkräften im Bereich der Cybersicherheit in der gesamten Union, einschließlich von geeignetem Personal für die Durchführung von Konformitätsbewertungen durch Dritte gemäß dieser Verordnung;***

***(f) die mögliche Notwendigkeit einer Änderung dieser Verordnung.***

***Die Expertengruppe soll auch Trends auf Ebene der Union und der Mitgliedstaaten in Bezug auf bestehende und gepatchte Schwachstellen erfassen.***

***3. Die Expertengruppe berücksichtigt die Ansichten eines breiten Spektrums von Interessengruppen.***

***4. Die Expertengruppe wird von der Kommission geleitet und gemäß den horizontalen Bestimmungen über die Einsetzung und Arbeitsweise von Expertengruppen der Kommission gebildet. In diesem Zusammenhang kann die Kommission auf Ad-hoc-Basis Experten mit spezifischem Fachwissen***

***einladen.***

***5. Die Expertengruppe erfüllt ihre Aufgaben nach dem Grundsatz***

***der Transparenz. Die Kommission veröffentlicht eine Zusammenfassung der Sitzungen der Sachverständigengruppe und andere relevante Dokumente auf der Website der Kommission.***

Oder. en

*Rechtfertigung*

*Die Konsultation der Interessengruppen wird für das Funktionieren dieser Verordnung von wesentlicher Bedeutung sein. Deshalb sollte die Kommission die Expertengruppe für die Widerstandsfähigkeit im Internet einsetzen und umfassend konsultieren.*

**Abänderung 54**

**Vorschlag für eine Verordnung Artikel 9 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***Artikel 9a*** |
| | ***Öffentliche Beschaffung von Produkten mit digitalen Elementen*** |
| | ***1. Unbeschadet der Richtlinien 2014/24/EU[1] und 2014/25/EU2 des Europäischen Parlaments und des Rates gewährleisten die Mitgliedstaaten bei der Beschaffung von Produkten mit digitalen Elementen ein hohes Maß an Cybersicherheit und eine angemessene erwartete Produktlebensdauer.*** |
| | ***2. Die Mitgliedstaaten stellen sicher, dass die Hersteller Schwachstellen in öffentlich beschafften Produkten mit digitalen Elementen unverzüglich beheben, unter anderem durch die unverzügliche Bereitstellung von Sicherheitsupdates.*** |

***[1] Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über öffentliche Aufträge und zur Aufhebung der***

***Richtlinie 2004/18/EG Text von Bedeutung für den EWR (ABl. L 94 vom 28.3.2014, S. 65).***

***[2] Richtlinie 2014/25/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die Auftragsvergabe durch***

***Auftraggeber im Bereich der Wasser-, Energie- und Verkehrsversorgung sowie der Postdienste und zur Aufhebung der Richtlinie 2004/17/EG Text von Bedeutung für den EWR (ABl. L 94 vom 28.3.2014, S. 243).***

Oder. en

*Rechtfertigung*

*Es ist von entscheidender Bedeutung, dass die Mitgliedstaaten der Cybersicherheit im öffentlichen Auftragswesen Vorrang einräumen.*

**Abänderung 55**

**Vorschlag für eine Verordnung Artikel 10 - Absatz 4**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 4. (2) Um der Verpflichtung nach Absatz 1 nachzukommen, lassen die Hersteller beim Einbau von Komponenten, die von Dritten bezogen werden, in Produkte mit digitalen Elementen die erforderliche Sorgfalt walten. Sie stellen sicher, dass diese Komponenten die Sicherheit des Produkts mit digitalen Bestandteilen nicht beeinträchtigen. | (4) Um der Verpflichtung nach Absatz 1 nachzukommen, lassen die Hersteller beim Einbau von Komponenten, die von Dritten bezogen werden, in Produkte mit digitalen Elementen die erforderliche Sorgfalt walten. Sie stellen sicher, dass diese Komponenten die Sicherheit des Produkts mit digitalen Bestandteilen nicht beeinträchtigen. ***Bei der Integration von Komponenten von Open-Source-Software, die nicht im Rahmen einer gewerblichen Tätigkeit in Verkehr gebracht wurden, stellen die Hersteller sicher, dass diese Komponenten mit dieser Verordnung übereinstimmen.*** |

Oder. en

**Abänderung 56**

**Vorschlag für eine**

**Verordnung**

**Artikel 10 - Absatz 6 - Unterabsatz 1**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
| --- | --- |
| Wenn ein Produkt mit digitalen Elementen auf den Markt gebracht wird, ***und für*** die | Wenn ein Produkt mit digitalen Elementen auf den Markt gebracht wird, müssen die ***Hersteller*** |

| | |
|---|---|
| Während der voraussichtlichen Lebensdauer des Produkts ***oder während eines Zeitraums von fünf Jahren nach dem Inverkehrbringen des Produkts, je nachdem, welcher Zeitraum kürzer ist,*** stellen die Hersteller sicher, dass Schwachstellen des Produkts wirksam und in Übereinstimmung mit den grundlegenden Anforderungen in Anhang I Abschnitt 2 behandelt werden. | ***legt die erwartete Produktlebensdauer dieser Produkte fest. Dabei stellt der Hersteller sicher, dass*** die erwartete Produktlebensdauer ***den angemessenen Erwartungen der Verbraucher entspricht und dass sie die Nachhaltigkeit und die Notwendigkeit der Gewährleistung langlebiger Produkte mit digitalen Elementen fördert. Die*** Hersteller stellen sicher, dass Schwachstellen dieses Produkts ***zumindest während der voraussichtlichen Lebensdauer des Produkts*** wirksam und im Einklang mit den in Anhang I Abschnitt 2 festgelegten grundlegenden Anforderungen behandelt werden. ***Gegebenenfalls ist die voraussichtliche Produktlebensdauer auf dem Produkt oder seiner Verpackung deutlich anzugeben oder in die vertraglichen Vereinbarungen aufzunehmen.*** |

Oder. en

*Rechtfertigung*

*Aufgrund des horizontalen Charakters dieser Verordnung ist es schwierig, die erwartete Produktlebensdauer auf einen Mindest- oder Höchstzeitraum von Jahren festzulegen. Daher sollte der Hersteller die Möglichkeit haben, die erwartete Produktlebensdauer festzulegen, vorausgesetzt, sie entspricht den Erwartungen der Verbraucher und wird deutlich beworben.*

**Abänderung 57**

**Vorschlag für eine**

**Verordnung**
**Artikel 10 - Absatz 6 - Unterabsatz 2 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***Bei Business-to-Consumer-Produkten mit digitalen Elementen umfassen diese Verfahren gegebenenfalls standardmäßig automatische Sicherheitsaktualisierungen. Die Nutzer sollten weiterhin die Möglichkeit haben, diese automatischen Sicherheitsaktualisierungen zu*** |

***deaktivieren.***

Oder. en

*Rechtfertigung*

*Sicherheitsaktualisierungen sollten nach Möglichkeit automatisch installiert werden.*

**Abänderung 58**

**Vorschlag für eine Verordnung**
**Artikel 10 - Absatz 6 - Unterabsatz 2 b (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***Die Hersteller informieren die Nutzer aktiv darüber, wenn ihr Produkt mit digitalen Elementen das Ende der erwarteten Produktlebensdauer erreicht hat und die Anforderungen an den Umgang mit Sicherheitsrisiken nicht mehr gelten.*** |

Oder. en

**Abänderung 59**

**Vorschlag für eine**

**Verordnung**
**Artikel 10 - Absatz 6 - Unterabsatz 2 c (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***Ist die voraussichtliche Lebensdauer eines Produkts kürzer als fünf Jahre und ist daher die Behandlung von Sicherheitslücken gemäß den in Anhang I Abschnitt 2 festgelegten Anforderungen an die Behandlung von Sicherheitslücken beendet, so gewähren die Hersteller den Unternehmen freien Zugang zum Quellcode eines solchen Produkts mit digitalen Elementen. Diese Unternehmen verpflichten sich, die Bereitstellung von Diensten zur Behebung von Sicherheitslücken, insbesondere von Sicherheitsaktualisierungen, auszuweiten. Der Zugang zu solchen Quellcodes wird nur gewährt, wenn dies in einer vertraglichen Vereinbarung vorgesehen ist. Diese Vereinbarungen müssen das Eigentum an dem Produkt mit digitalen Elementen schützen und die*** |

***Verbreitung des Quellcodes an die Öffentlichkeit verhindern. Die Verpflichtung, kostenlosen Zugang zum Quellcode zu gewähren, entfällt, wenn die Lebensdauer des Produkts fünf Jahre erreicht hat.***

Oder. en

**Abänderung 60**

**Vorschlag für eine**
**Verordnung Artikel 10 -**
**Absatz 8**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (8) Die Hersteller halten die technischen Unterlagen und die EU-Konformitätserklärung, soweit einschlägig, zehn Jahre lang nach dem Inverkehrbringen des Produkts mit digitalen Elementen für die Marktüberwachungsbehörden bereit. | 8. Die Hersteller halten die technischen Unterlagen und gegebenenfalls die EU-Konformitätserklärung nach dem Inverkehrbringen des Produkts mit digitalen Elementen zehn Jahre lang ***oder über die voraussichtliche Lebensdauer des Produkts, je nachdem, welcher Zeitraum länger ist, für die*** Marktaufsichtsbehörden bereit. |

Oder. en

**Abänderung 61**

**Vorschlag für eine**

**Verordnung**
**Artikel 10 - Absatz 10 - Unterabsatz 1 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***Werden diese Informationen und Anleitungen in elektronischer Form bereitgestellt, so müssen die Hersteller:*** |
| | ***(a) sie in einem benutzerfreundlichen Format präsentieren, das es dem Nutzer ermöglicht, sie online zu konsultieren, herunterzuladen, auf einem elektronischen Gerät zu speichern und auszudrucken;*** |
| | ***(b) sicherstellen, dass sie während der voraussichtlichen Lebensdauer des Produkts mit digitalen Elementen online zugänglich sind.*** |

Oder. en

*Rechtfertigung*

*Die Informationen und Anweisungen für die Nutzer sollten so benutzerfreundlich wie möglich sein.*

**Abänderung 62**

**Vorschlag für eine**
**Verordnung Artikel 10 -**
**Absatz 12**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (12) Ab dem Inverkehrbringen und während der voraussichtlichen Lebensdauer des Produkts ***oder während eines Zeitraums von fünf Jahren nach dem Inverkehrbringen eines Produkts mit digitalen Elementen, je nachdem, welcher Zeitraum kürzer ist,*** ergreift der Hersteller, wenn er weiß oder Grund zu der Annahme hat, dass das Produkt mit digitalen Elementen oder die vom Hersteller eingerichteten Verfahren nicht den in Anhang I aufgeführten grundlegenden Anforderungen entsprechen, unverzüglich die erforderlichen Korrekturmaßnahmen, um die Konformität des Produkts mit digitalen Elementen oder der Verfahren des Herstellers herzustellen, das Produkt zurückzunehmen oder zurückzurufen, je nachdem, was angemessen ist. | (12) Ab dem Inverkehrbringen und während der voraussichtlichen Lebensdauer des Produkts ergreift ein Hersteller, der weiß oder Grund zu der Annahme hat, dass das Produkt mit digitalen Elementen oder die vom Hersteller eingerichteten Verfahren nicht den wesentlichen Anforderungen in Anhang I entsprechen, unverzüglich die erforderlichen Korrekturmaßnahmen, um die Konformität des Produkts mit digitalen Elementen oder der Verfahren des Herstellers herzustellen, es gegebenenfalls zurückzunehmen oder zurückzurufen. |

Oder. en

*Rechtfertigung*

*Erforderlich zur Anpassung an die neue Definition der erwarteten Produktlebensdauer.*

**Abänderung 63**

**Vorschlag für eine**

**Verordnung**
**Artikel 10 - Absatz 15**

| *Von der Kommission vorgeschlagener Text* | *Abänderun* |
|---|---|
| *g* | |

(15) Die Kommission ***kann im Wege von Durchführungsrechtsakten*** das Format und die Bestandteile der Software-Materialliste gemäß Anhang I Abschnitt 2 Nummer 1 festlegen. ***Diese Durchführungsrechtsakte werden nach dem in Artikel 51 Absatz 2 genannten Prüfverfahren erlassen.***

15. Der Kommission ***wird die Befugnis übertragen, delegierte Rechtsakte gemäß Artikel 50 zu erlassen, um*** das Format und die Bestandteile der Software-Materialliste gemäß Anhang I Abschnitt 2 Nummer 1 festzulegen.

Oder. en

**Abänderung 64**

**Vorschlag für eine Verordnung Artikel 11 - Absatz 1**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 1. Der Hersteller meldet der ENISA unverzüglich, auf ***jeden Fall aber innerhalb von 24 Stunden, nachdem er davon Kenntnis erlangt hat,*** jede aktiv ausgenutzte Sicherheitslücke in einem Produkt mit digitalen Elementen***. Die Meldung muss Einzelheiten zu dieser Schwachstelle und gegebenenfalls zu den getroffenen Abhilfemaßnahmen enthalten***. Die ENISA leitet die Meldung unverzüglich nach Erhalt an das CSIRT weiter, das für die Zwecke der koordinierten Offenlegung von Schwachstellen gemäß Artikel [Artikel X] der ***Richtlinie [Richtlinie XXX/XXXX (NIS2)]*** des betreffenden Mitgliedstaats benannt wurde, es sei denn, es liegen berechtigte Gründe im Zusammenhang mit Cybersicherheitsrisiken vor, und unterrichtet die Marktaufsichtsbehörde über die gemeldete Schwachstelle. | 1. Der Hersteller meldet der ENISA jede aktiv ausgenutzte Sicherheitslücke, die in dem Produkt mit digitalen Elementen ***gemäß Absatz 1a dieses Artikels*** enthalten ist. Die ENISA leitet die Meldung unverzüglich nach Erhalt an das CSIRT weiter, das für die Zwecke der koordinierten Offenlegung von Sicherheitslücken gemäß Artikel [Artikel X] der ***Richtlinie (EU) 2022/2555*** des betreffenden Mitgliedstaats benannt wurde, es sei denn, es liegen berechtigte Gründe im Zusammenhang mit Cybersicherheitsrisiken vor, und unterrichtet die Marktüberwachungsbehörde über die gemeldete Sicherheitslücke. Stehen für ***eine gemeldete Schwachstelle keine Abhilfemaßnahmen zur Verfügung, stellt die ENISA sicher, dass die Informationen über die gemeldete Schwachstelle im Einklang mit strengen Sicherheitsprotokollen und nach dem Grundsatz "Kenntnis nur, wenn nötig" weitergegeben werden.*** |

Oder. en

*Rechtfertigung*

*Der Zeitplan für die Berichterstattung und die darin aufzunehmenden Informationen sind auf die NIS 2 abgestimmt (Absatz 1a). Es sollten sichere Protokolle vorhanden sein, um sicherzustellen, dass Informationen über nicht behobene Schwachstellen nicht verbreitet werden, um weitere Risiken für die Cybersicherheit zu vermeiden.*

**Abänderung 65**

**Vorschlag für eine**

**Verordnung**
**Artikel 11 - Absatz 1 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
| --- | --- |
| | ***(1a) Die in Absatz 1 genannten Meldungen unterliegen dem folgenden Verfahren:*** |
| | ***(a) eine frühzeitige Warnung, ohne unnötige Verzögerung und auf jeden Fall innerhalb von 24 Stunden, nachdem der Hersteller von der aktiv ausgenutzten Schwachstelle Kenntnis erlangt hat, mit der Angabe, ob es bekannte Abhilfemaßnahmen oder Maßnahmen zur Schadensbegrenzung gibt;*** |
| | ***(b) unverzüglich, auf jeden Fall aber innerhalb von 72 Stunden, nachdem der Hersteller von der aktiv ausgenutzten Schwachstelle Kenntnis erlangt hat, eine Meldung über die Schwachstelle, in der gegebenenfalls die unter Buchstabe a genannten Informationen aktualisiert werden, alle getroffenen Korrektur- oder Abhilfemaßnahmen im Einzelnen aufgeführt werden und eine Bewertung des Ausmaßes der Schwachstelle, einschließlich ihres Schweregrads und ihrer Auswirkungen, angegeben wird;*** |
| | ***(c) auf Ersuchen der ENISA einen Zwischenbericht über relevante Aktualisierungen des Status;*** |
| | ***(d) innerhalb eines Monats nach Übermittlung der Schwachstellenmeldung gemäß Buchstabe b) einen Abschlussbericht, der mindestens Folgendes enthält*** |
| | ***(i) eine detaillierte Beschreibung der Schwachstelle, einschließlich ihres Schweregrads und ihrer Auswirkungen;*** |
| | ***(ii) soweit verfügbar, Informationen über jeden Akteur, der die Schwachstelle ausgenutzt hat oder ausnutzt;*** |
| | ***(iii) Einzelheiten über das Sicherheitsupdate oder andere Abhilfemaßnahmen, die zur Behebung der Schwachstelle zur Verfügung gestellt*** |

***wurden.***

Oder. en

*Rechtfertigung*

*Angleichung an die NIS 2.*

**Abänderung 66**

**Vorschlag für eine Verordnung**
**Artikel 11 - Absatz 1 b (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(1b) Nachdem ein Sicherheitsupdate zur Verfügung gestellt oder eine andere Form von Korrektur- oder Abhilfemaßnahmen ergriffen wurde, nimmt die ENISA die gemäß Absatz 1 gemeldete Schwachstelle in die in Artikel 12 der Richtlinie (EU) 2022/2555 genannte europäische Datenbank für Sicherheitsrisiken auf.*** |

Oder. en

*Rechtfertigung*

*Es ist wichtig, dass die ENISA die Schwachstellendatenbank mit Informationen über alle bekannten Schwachstellen, die gepatcht werden können, aktualisiert.*

**Abänderung 67**

**Vorschlag für eine Verordnung Artikel 11 - Absatz 2**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 2. Der Hersteller meldet der ENISA ***unverzüglich und in jedem Fall innerhalb von 24 Stunden, nachdem er davon Kenntnis erlangt hat,*** jeden Vorfall, der sich auf die Sicherheit des Produkts mit digitalen Elementen auswirkt. Die ENISA leitet die Meldungen unverzüglich an die gemäß Artikel [Artikel X] der ***Richtlinie [Richtlinie XXX/XXXX (NIS2)]*** der betreffenden Mitgliedstaaten benannte zentrale Kontaktstelle weiter und unterrichtet die Marktüberwachungsbehörde über die gemeldeten Vorfälle, es sei denn, es liegen berechtigte Gründe für ein | Cybersicherheitsrisiko vor. Die Störungsmeldung ***enthält Informationen über die Schwere und die Auswirkungen der Störung und, sofern*** |

2. Der Hersteller meldet der ENISA alle ***bedeutenden*** Vorfälle, die sich auf die Sicherheit des Produkts mit digitalen Elementen auswirken, gemäß ***Absatz 2b dieses Artikels***. Die ENISA leitet die Meldungen unverzüglich an die gemäß Artikel [Artikel X] der ***Richtlinie (EU) 2022/2555*** der betreffenden Mitgliedstaaten benannte zentrale Kontaktstelle weiter und unterrichtet die Marktüberwachungsbehörde über die gemeldeten ***bedeutsamen Vorkommnisse***, es sei denn, es liegen berechtigte Gründe im Zusammenhang mit Cybersicherheitsrisiken vor. Die ***bloße*** Meldung ***unterwirft die meldende Stelle nicht einer erhöhten Haftung***.

***Gegebenenfalls ist anzugeben, ob der Hersteller vermutet, dass der Vorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder ob er grenzüberschreitende Auswirkungen hat.***

Oder. en

*Rechtfertigung*

*In Anlehnung an die NIS 2 sollten nur schwerwiegende Vorfälle obligatorisch gemeldet werden. Auch der Zeitplan muss angepasst werden (Absatz 2b).*

**Abänderung 68**

**Vorschlag für eine**

**Verordnung**
**Artikel 11 - Absatz 2 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***2a. Ein Ereignis gilt als signifikant im Sinne von Absatz 2, wenn:*** |
| | ***(a) sie eine schwerwiegende Betriebsstörung der Produktion oder der Dienstleistungen für den betreffenden Hersteller verursacht hat oder verursachen kann, die sich auf die Sicherheit eines Produkts auswirken würde; oder*** |
| | ***(b) sie andere natürliche oder juristische Personen durch die Verursachung eines erheblichen materiellen oder immateriellen Schadens beeinträchtigt hat oder beeinträchtigen kann.*** |

Oder. en

*Rechtfertigung*

*Angleichung an die NIS2-Definition des Begriffs "bedeutendes Ereignis". Um keine Überlastung zu verursachen*
*Hersteller oder auch die ENISA, sollten nur wesentliche Vorfälle, die die Sicherheit des Produkts betreffen, obligatorisch gemeldet werden.*

**Abänderung 69**

**Vorschlag für eine**

**Verordnung**
**Artikel 11 - Absatz 2 b (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(2b) Für die Meldungen nach Absatz 2 gilt das folgende Verfahren:*** |
| | ***(a) eine frühzeitige Warnung, ohne unnötige Verzögerung und in jedem Fall innerhalb von 24 Stunden, nachdem der Hersteller von dem bedeutsamen Vorkommnis Kenntnis erlangt hat, aus der gegebenenfalls hervorgeht, ob der Verdacht besteht, dass das bedeutende Vorkommnis durch rechtswidrige oder böswillige Handlungen verursacht wurde oder grenzüberschreitende Auswirkungen haben könnte;*** |
| | ***(b) unverzüglich, auf jeden Fall aber innerhalb von 72 Stunden, nachdem der Hersteller von dem bedeutsamen Vorkommnis Kenntnis erlangt hat, eine Meldung über das Vorkommnis, in der gegebenenfalls die unter Buchstabe a genannten Informationen aktualisiert werden und eine erste Bewertung des bedeutsamen Vorkommnisses, einschließlich der Schwere und der Auswirkungen, sowie, soweit verfügbar, die Indikatoren für eine Kompromittierung angegeben werden;*** |
| | ***(c) auf Ersuchen der ENISA einen Zwischenbericht über relevante Aktualisierungen des Status;*** |
| | ***(d) innerhalb eines Monats nach Übermittlung der Meldung des Vorfalls gemäß Buchstabe b) einen Abschlussbericht, der mindestens Folgendes enthält*** |
| | ***(i) eine detaillierte Beschreibung des Vorfalls, einschließlich seiner Schwere und seiner Auswirkungen;*** |
| | ***(ii) die Art der Bedrohung oder die Grundursache, die den Vorfall wahrscheinlich ausgelöst hat;*** |
| | ***(iii) angewandte und laufende Abhilfemaßnahmen;*** |

***(iv) ggf. die grenzüberschreitenden Auswirkungen des Vorfalls;***

***Ist ein Vorfall zum Zeitpunkt der Vorlage des Abschlussberichts gemäß Unterabsatz 1 Buchstabe d noch nicht abgeschlossen, stellen die Mitgliedstaaten sicher, dass die betroffenen Einrichtungen eine***

| | |
|---|---|
| | ***zu diesem Zeitpunkt einen Fortschrittsbericht und innerhalb eines Monats einen Abschlussbericht über den Umgang mit dem Vorfall.*** |

Oder. en

*Rechtfertigung*

*Angleichung an die NIS 2.*

**Abänderung 70**

**Vorschlag für eine Verordnung Artikel 11 - Absatz 4**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 4. Der Hersteller unterrichtet die Nutzer des Produkts mit digitalen Elementen unverzüglich nach Bekanntwerden über die Störung und erforderlichenfalls über Korrekturmaßnahmen, die der Nutzer ergreifen kann, um die Auswirkungen der Störung zu mindern. | 4. Der Hersteller informiert die Nutzer des Produkts mit digitalen Elementen unverzüglich nach Bekanntwerden über das ***signifikante*** Vorkommnis und erforderlichenfalls über Abhilfemaßnahmen, die der Nutzer ergreifen kann, um die Auswirkungen des ***signifikanten*** Vorkommnisses zu mindern. |

Oder. en

**Abänderung 71**

**Vorschlag für eine**

**Verordnung**
**Artikel 11 - Absatz 4 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(4a) Die ENISA stellt sicher, dass die Meldungen nach den Absätzen 1 und 2 über Kommunikationskanäle übermittelt und auf Servern gespeichert werden, die das höchstmögliche Maß an Cybersicherheit und Schutz vor böswilligen Akteuren gewährleisten.*** |

Oder. en

**Abänderung 72**

**Vorschlag für eine Verordnung Artikel 11 - Absatz 5**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 5. (3) Die Kommission ***kann im Wege von Durchführungsrechtsakten*** die Art der Informationen, das ***Format und das Verfahren*** für die gemäß den Absätzen 1 und 2 übermittelten Mitteilungen näher festlegen. Diese Durchführungsrechtsakte werden nach dem ***in Artikel 51 Absatz 2 genannten Prüfverfahren*** erlassen. | 5. (3) Die Kommission ***erlässt delegierte Rechtsakte gemäß Artikel 50, um das Format und das Verfahren sowie gegebenenfalls*** die Art der Informationen für die gemäß den Absätzen 1 und 2 übermittelten Meldungen näher festzulegen. Diese ***delegierten*** Rechtsakte werden ***bis zum ... [12 Monate nach Inkrafttreten dieser Verordnung] erlassen***. |

Oder. en

**Abänderung 73**

**Vorschlag für eine Verordnung Artikel 11 - Absatz 6**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 6. (3) Auf der Grundlage der gemäß den Absätzen 1 und 2 eingegangenen Meldungen erstellt die ENISA alle zwei Jahre einen technischen Bericht über sich abzeichnende Trends bei den Cybersicherheitsrisiken von Produkten mit digitalen Elementen und legt ihn der in Artikel [Artikel X] der *Richtlinie [Richtlinie XXX/XXXX (NIS2)]* genannten Kooperationsgruppe vor. Der erste dieser Berichte wird innerhalb von 24 Monaten nach Beginn der Anwendung der in den Absätzen 1 und 2 festgelegten Verpflichtungen vorgelegt. | 6. (3) Die ENISA erstellt auf der Grundlage der gemäß den Absätzen 1 und 2 eingegangenen Meldungen alle zwei Jahre einen technischen Bericht über sich abzeichnende Trends bei den Cybersicherheitsrisiken von Produkten mit digitalen Elementen und legt ihn der in Artikel [Artikel X] der ***Richtlinie (EU) 2022/2555*** genannten Kooperationsgruppe vor. Der erste dieser Berichte wird innerhalb von 24 Monaten nach Beginn der Anwendung der in den Absätzen 1 und 2 festgelegten Verpflichtungen vorgelegt. ***Die ENISA nimmt relevante Informationen aus ihren technischen Berichten in ihren Bericht über den Stand der Cybersicherheit in der Union*** |

***gemäß Artikel 18 der Richtlinie (EU) 2022/2555 auf.***

Oder. en

**Abänderung 74**

**Vorschlag für eine**
**Verordnung Artikel 11 a**
**(neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***Artikel 11a*** |
| | ***Freiwillige*** |
| | ***Berichterstattung*** |
| | ***1. Zusätzlich zu den in Artikel 11 festgelegten Meldepflichten können der ENISA auf freiwilliger Basis Meldungen von folgenden Personen übermittelt werden:*** |
| | ***(a) Hersteller in Bezug auf Zwischenfälle, Cyber-Bedrohungen und Beinahe-Unfälle;*** |
| | ***(b) andere als die unter Buchstabe a genannten Stellen, unabhängig davon, ob sie in den Anwendungsbereich dieser Verordnung fallen, in Bezug auf signifikante und nicht signifikante Vorfälle, Cyberbedrohungen und Beinaheunfälle;*** |
| | ***(c) jeden Akteur in Bezug auf Schwachstellen, die in die in Artikel 12 der Verordnung 2022/255 genannte europäische Schwachstellendatenbank aufgenommen werden können.*** |
| | ***2. Die ENISA bearbeitet die in Absatz 1a des vorliegenden Artikels genannten Meldungen nach dem Verfahren des Artikels 11. Die ENISA kann der Bearbeitung von Pflichtmeldungen Vorrang vor freiwilligen Meldungen einräumen.*** |
| | ***3. Gegebenenfalls stellt die ENISA die Vertraulichkeit und den angemessenen Schutz der von der meldenden Stelle übermittelten Informationen sicher. Unbeschadet der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten darf die*** |

***freiwillige Meldung nicht dazu führen, dass der meldenden Stelle zusätzliche Verpflichtungen auferlegt werden, die ihr nicht auferlegt worden wären, wenn sie die Meldung nicht eingereicht hätte.***

Oder. en

**Abänderung 75**

**Vorschlag für eine Verordnung Artikel 14 - Absatz 3**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 3. Ist ein Händler der Auffassung oder hat er Grund zu der Annahme, dass ein Produkt mit digitalen Elementen oder die vom Hersteller eingerichteten Verfahren nicht mit den in Anhang I aufgeführten grundlegenden Anforderungen übereinstimmen, stellt er das Produkt mit digitalen Elementen erst dann auf dem Markt bereit, wenn die Konformität des Produkts oder der vom Hersteller eingerichteten Verfahren hergestellt ist. Stellt das Produkt mit digitalen Elementen ein erhebliches Cybersicherheitsrisiko dar, unterrichtet der Händler den Hersteller und die Marktüberwachungsbehörden darüber. | 3. Ist ein Händler der Auffassung oder hat er aufgrund der ihm vorliegenden ***Informationen*** Grund zu der Annahme, dass ein Produkt mit digitalen Elementen oder die vom Hersteller eingerichteten Verfahren nicht mit den in Anhang I aufgeführten grundlegenden Anforderungen übereinstimmen, stellt er das Produkt mit digitalen Elementen erst dann auf dem Markt bereit, wenn die Konformität des Produkts oder der vom Hersteller eingerichteten Verfahren hergestellt ist. Stellt das Produkt mit digitalen Elementen ein erhebliches Cybersicherheitsrisiko dar, unterrichtet der Händler den Hersteller und die Marktüberwachungsbehörden darüber. |

Oder. en

*Rechtfertigung*

*Bei den Händlern handelt es sich häufig um Kleinstunternehmen oder KMU. Sie sollten nicht verpflichtet sein, die Konformität von Produkten proaktiv zu prüfen.*

**Abänderung 76**

**Vorschlag für eine**

**Verordnung**
**Artikel 14 - Absatz 4 - Unterabsatz 1**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| Händler, die wissen oder Grund zu der Annahme haben, dass ein Produkt mit digitalen Elementen, das sie auf dem | Markt bereitgestellt haben, oder die vom Hersteller eingerichteten Verfahren nicht konform sind |

| | |
|---|---|
| Händler, die wissen oder aufgrund der ihnen ***vorliegenden Informationen*** Grund zu der Annahme haben, dass ein Produkt mit digitalen Elementen, das sie auf dem Markt bereitgestellt haben, oder die eingerichteten Verfahren | |

| | |
|---|---|
| mit den grundlegenden Anforderungen in Anhang I stellt sicher, dass die erforderlichen Korrekturmaßnahmen ergriffen werden, um die Konformität des Produkts mit den digitalen Elementen oder den vom Hersteller eingerichteten Verfahren herzustellen oder um das Produkt gegebenenfalls zurückzunehmen oder zurückzurufen. | nicht mit den grundlegenden Anforderungen in Anhang I übereinstimmen, stellen sicher, dass die erforderlichen Korrekturmaßnahmen ergriffen werden, um die Konformität des Produkts mit den digitalen Elementen oder den vom Hersteller eingerichteten Verfahren herzustellen oder das Produkt gegebenenfalls zurückzunehmen oder zurückzurufen. |

Oder. en

*Rechtfertigung*

*Bei den Händlern handelt es sich häufig um Kleinstunternehmen oder KMU. Sie sollten nicht verpflichtet sein, die Konformität von Produkten proaktiv zu prüfen.*

**Abänderung 77**

**Vorschlag für eine Verordnung Artikel 14 - Absatz 6**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (6) Erhält der Händler eines Produkts mit digitalen Elementen Kenntnis davon, dass der Hersteller dieses Produkts seine Tätigkeit eingestellt hat und infolgedessen nicht in der Lage ist, den in dieser Verordnung festgelegten Verpflichtungen nachzukommen, informiert der Händler die zuständigen Marktüberwachungsbehörden über diese Situation sowie - soweit möglich - die Nutzer der in Verkehr gebrachten Produkte mit digitalen Elementen mit allen verfügbaren Mitteln. | 6. Stellt der Händler eines Produkts mit digitalen Bestandteilen ***auf der Grundlage der ihm vorliegenden Informationen fest,*** dass der Hersteller dieses Produkts seinen Betrieb eingestellt hat und infolgedessen nicht in der Lage ist, die in dieser Verordnung festgelegten Verpflichtungen zu erfüllen, so unterrichtet er die zuständigen Marktüberwachungsbehörden sowie - soweit möglich - die Nutzer der in Verkehr gebrachten Produkte mit digitalen Bestandteilen mit allen ihm zur Verfügung stehenden Mitteln über diesen Sachverhalt. |

Oder. en

*Rechtfertigung*

*Die Händler sind häufig Kleinstunternehmen oder KMU. Sie wissen oft nicht, ob ein Hersteller seinen Betrieb eingestellt hat.*

**Abänderung 78**

**Vorschlag für eine Verordnung Artikel 17 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***Artikel 17a*** |
| | ***Leitlinien*** |
| | ***1. Um Klarheit und Sicherheit für die Wirtschaftsbeteiligten und Kohärenz zwischen ihren Praktiken zu schaffen, erstellt und veröffentlicht die Kommission Leitlinien in Form eines Handbuchs für die Wirtschaftsbeteiligten, in dem erläutert wird, wie diese Verordnung anzuwenden ist, wobei der Schwerpunkt darauf liegt, wie Kleinst-, kleinen und mittleren Unternehmen die Einhaltung der Verordnung erleichtert werden kann.*** |
| | ***2. Die Leitlinien werden bis zum ... [12 Monate nach Inkrafttreten dieser Verordnung] veröffentlicht und regelmäßig aktualisiert, insbesondere im Hinblick auf mögliche Änderungen der Liste der kritischen Produkte in Anhang III. Sie enthalten mindestens die folgenden Elemente:*** |
| | ***(a) eine ausführliche Erläuterung des Anwendungsbereichs dieser Verordnung, in der die Auswirkungen auf die verschiedenen Wirtschaftssektoren der Union dargelegt werden;*** |
| | ***(b) klare und anschauliche Beispiele von Lösungen für die Datenfernverarbeitung, die vom Hersteller oder in seinem Auftrag entworfen und entwickelt wurden;*** |
| | ***(c) Informationen, um zu bestimmen, was eine kommerzielle Tätigkeit für Entwickler freier und quelloffener Software darstellt;*** |
| | ***(d) eine ausführliche Beschreibung der Methodik, die zur Unterscheidung zwischen kritischen*** |

***Produkten mit digitalen Elementen der Klassen I und II angewandt wird;***

***(e) eine klare Veranschaulichung der Wechselwirkung zwischen dieser Verordnung und anderem Unionsrecht, insbesondere in Bezug auf die Konformitätsvermutung und***

***Konformitätsbewertungen;***

***(f) Leitlinien für die Hersteller zur Durchführung der in Artikel 10 Absatz 2 genannten Risikobewertung im Bereich der Cybersicherheit sowie eine Erläuterung, wie sich die Risikobewertung auf die Einhaltung der grundlegenden Anforderungen dieser Verordnung durch die Hersteller auswirkt;***

***(g) Leitlinien für die Hersteller zur angemessenen Bestimmung der erwarteten Produktlebensdauer mit einem angemessenen Grad an Produktgranularität;***

***(h) eine Erläuterung, wie mit den Meldepflichten nach dieser Verordnung oder nach anderem Unionsrecht umzugehen ist;***

***(i) einen Überblick über die Befugnisse der Kommission zum Erlass von delegierten Rechtsakten und Durchführungsrechtsakten, gegebenenfalls mit Angabe der entsprechenden Fristen.***

***3. Bei der Ausarbeitung der Leitlinien gemäß diesem Artikel konsultiert die Kommission die Sachverständigengruppe.***

Oder. en

*Rechtfertigung*

*Diese horizontale Verordnung ist sehr komplex, insbesondere für KMU. Die Kommission sollte die Unternehmen umfassend unterstützen, indem sie ihnen unter anderem Leitlinien und Orientierungshilfen für die Anwendung dieser Verordnung an die Hand gibt.*

**Abänderung 79**

**Vorschlag für eine Verordnung Artikel 19 - Absatz 1**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|

***Gibt es keine harmonisierten Normen gemäß Artikel 18 oder ist*** die Kommission ***der Auffassung, dass die einschlägigen harmonisierten Normen nicht ausreichen, um die*** Anforderungen ***dieser Verordnung zu erfüllen oder dem Normungsauftrag der Kommission*** nachzukommen***, oder gibt es***

***1.*** Der Kommission ***wird die Befugnis übertragen, gemäß Artikel 50 delegierte Rechtsakte zu erlassen, um gemeinsame Spezifikationen für technische*** Anforderungen ***festzulegen, mit denen*** die ***Anforderungen des Anhangs I für Produkte, die in den Anwendungsbereich dieser Verordnung fallen,*** erfüllt werden können.

***Kommt es zu unangemessenen Verzögerungen im Normungsverfahren oder wurde*** der ***Antrag der*** Kommission ***auf harmonisierte Normen von den*** europäischen Normungsorganisationen ***nicht angenommen, so wird die Kommission ermächtigt, im Wege von Durchführungsrechtsakten gemeinsame Spezifikationen für die*** grundlegenden Anforderungen des Anhangs I ***zu erlassen. Diese Durchführungsrechtsakte werden*** nach ***dem in Artikel 51 Absatz 2 genannten Prüfverfahren erlassen***.

***Verordnung***, wenn die ***folgenden Bedingungen erfüllt sind:***

***(a)*** die Kommission eine ***oder mehrere*** europäische Normungsorganisationen ***gemäß Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1025/2012 aufgefordert hat, eine harmonisierte Norm für die*** in Anhang I aufgeführten grundlegenden Anforderungen zu ***erarbeiten, und dem Antrag nicht stattgegeben wurde oder die europäischen Normungsprodukte, die diesem Antrag entsprechen, nicht innerhalb der*** gemäß ***Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1025/2012 gesetzten Frist geliefert wurden oder die europäischen Normungsprodukte dem Antrag nicht entsprechen; und***

***(b) im Amtsblatt der Europäischen Union kein Verweis auf harmonisierte Normen, die die einschlägigen grundlegenden Anforderungen des Anhangs I abdecken, gemäß der Verordnung (EU) Nr. 1025/2012 veröffentlicht wurde und die Veröffentlichung eines solchen Verweises innerhalb eines angemessenen Zeitraums nicht zu erwarten ist.***

***2. Vor der Ausarbeitung des delegierten Rechtsakts teilt die Kommission der Sachverständigengruppe mit, dass sie der Auffassung ist, dass die Bedingungen in Absatz 1 erfüllt sind. Bei der Ausarbeitung der delegierten Rechtsakte trägt die Kommission den Stellungnahmen der Sachverständigengruppe Rechnung.***

***3. Wird eine harmonisierte Norm***

***von einer europäischen Normungsorganisation angenommen und der Kommission zur Veröffentlichung ihrer Fundstelle im Amtsblatt der Europäischen Union vorgeschlagen, so wird die Kommission***

| | |
|---|---|
| | ***die harmonisierte Norm im Einklang mit der Verordnung (EU) Nr. 1025/2012 zu bewerten. (2) Wenn die Bezugnahme auf eine harmonisierte Norm im Amtsblatt der Europäischen Union veröffentlicht wird, hebt die Kommission die in Absatz 1 genannten delegierten Rechtsakte oder die Teile davon auf, die dieselben in Anhang I aufgeführten grundlegenden Anforderungen abdecken.*** |

Oder. en

*Rechtfertigung*

*Gemeinsame Spezifikationen sollten für die Kommission nur eine letzte Option sein. Der Text steht weitgehend im Einklang mit der neuen Verordnung über die allgemeine Produktsicherheit.*

**Abänderung 80**

**Vorschlag für eine Verordnung Artikel 20 - Absatz 2**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (2) Die EU-Konformitätserklärung entspricht in ihrem Aufbau dem Muster in Anhang IV und enthält die in den einschlägigen Konformitätsbewertungsverfahren des Anhangs VI angegebenen Elemente. Diese Erklärung wird ständig aktualisiert. Sie wird in ***der/den*** Sprache***(n) zur*** Verfügung gestellt, ***die von dem Mitgliedstaat vorgeschrieben wird/werden***, in dem das Produkt mit digitalen Elementen in Verkehr gebracht oder bereitgestellt wird. | (2) Die EU-Konformitätserklärung entspricht in ihrem Aufbau dem Muster in Anhang IV und enthält die in den einschlägigen Konformitätsbewertungsverfahren des Anhangs VI angegebenen Elemente. Diese Erklärung wird ständig aktualisiert. Sie wird in ***einer*** Sprache zur Verfügung gestellt, die ***von den Behörden des*** Mitgliedstaats, in dem das Produkt mit digitalen Elementen in Verkehr gebracht oder bereitgestellt wird, ***leicht verstanden werden kann***. |

Oder. en

*Rechtfertigung*

*Es sollte vermieden werden, dass die Hersteller von Produkten mit digitalen Elementen, die oft eine grenzüberschreitende Dimension haben, die Erklärung in 24 verschiedenen Sprachen erstellen müssen.*

**Abänderung 81**

**Vorschlag für eine Verordnung Artikel 23 - Absatz 2**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (2) Die technischen Unterlagen sind vor dem Inverkehrbringen des Produkts mit digitalen Elementen zu erstellen und gegebenenfalls während der voraussichtlichen Lebensdauer des Produkts ***oder während eines Zeitraums von fünf Jahren nach dem Inverkehrbringen eines Produkts mit digitalen Elementen, je nachdem, welcher Zeitraum kürzer ist,*** kontinuierlich zu aktualisieren. | (2) Die technischen Unterlagen werden erstellt, bevor das Produkt mit digitalen Elementen in Verkehr gebracht wird, und werden gegebenenfalls während der voraussichtlichen Lebensdauer des Produkts laufend aktualisiert. |

Oder. en

*Rechtfertigung*

*Angleichung an die neue Definition der erwarteten Produktlebensdauer.*

**Abänderung 82**

**Vorschlag für eine Verordnung Artikel 23 - Absatz 5**

| *Von der Kommission vorgeschlagener Text* | *Abänderun g* |
|---|---|
| (5) Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte gemäß Artikel 50 zu erlassen, um diese Verordnung durch die Elemente zu ergänzen, die in die technischen Unterlagen gemäß Anhang V aufzunehmen sind, um den technologischen Entwicklungen sowie den bei der Durchführung dieser Verordnung eingetretenen Entwicklungen Rechnung zu tragen. | 5. Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte gemäß Artikel 50 zu erlassen, um diese Verordnung durch die Elemente zu ergänzen, die in die technischen Unterlagen gemäß Anhang V aufzunehmen sind, um technologischen Entwicklungen sowie Entwicklungen, die bei der Durchführung dieser Verordnung auftreten, Rechnung zu tragen. ***Die Kommission stellt sicher, dass der*** |

***Verwaltungsaufwand für Kleinstunternehmen sowie kleine und mittlere Unternehmen so gering wie möglich gehalten wird.***

Oder. en

**Abänderung 83**

**Vorschlag für eine Verordnung**
**Artikel 24 - Absatz 2 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(2a) Harmonisierte Normen, gemeinsame Spezifikationen oder europäische Cybersicherheitszertifizierungssysteme müssen sechs Monate lang in Kraft sein, bevor das in Absatz 2 genannte Konformitätsbewertungsverfahren angewandt wird. (2a) In den sechs Monaten vor der Anwendung von Absatz 2 oder in den Fällen, in denen aus Gründen, die eindeutig der Kommission zuzuschreiben sind, keine harmonisierten Normen, gemeinsamen Spezifikationen oder europäischen Cybersicherheitszertifizierungssysteme vorhanden sind, weisen die Hersteller die Konformität des kritischen Produkts mit den in Anhang III aufgeführten digitalen Elementen der Klasse I über das in Absatz 1 genannte Verfahren nach.*** |

Oder. en

*Rechtfertigung*

*Die Hersteller von kritischen Produkten der Klasse I sollten nicht durch das Fehlen von harmonisierte Normen, auch um einen übermäßigen Rückgriff auf Konformitätsbewertungen durch Dritte zu vermeiden, der zu Engpässen führen und Innovationen verzögern könnte. Wenn keine harmonisierten Normen, gemeinsamen Spezifikationen oder europäischen Zertifizierungssysteme für Cybersicherheit zur Verfügung stehen oder in den sechs Monaten nach ihrer Verabschiedung, können die Hersteller die Einhaltung dieser Verordnung im Rahmen des Selbstbewertungsverfahrens nachweisen.*

**Abänderung 84**

**Vorschlag für eine Verordnung Artikel 24 - Absatz 5**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|

| | |
|---|---|
| 5. Die benannten Stellen berücksichtigen die besonderen Interessen und Bedürfnisse kleiner und mittlerer Unternehmen ***(KMU)*** bei der Festsetzung der Gebühren für Konformitätsbewertungsverfahren und | 5. Die notifizierten Stellen berücksichtigen bei der Festsetzung der Gebühren für Konformitätsbewertungsverfahren die besonderen Interessen und Bedürfnisse von ***Kleinst-,*** kleinen und mittleren Unternehmen und senken diese Gebühren |

| | |
|---|---|
| diese Gebühren proportional zu ihren spezifischen Interessen und Bedürfnissen zu senken. | Gebühren, die ihren spezifischen Interessen und Bedürfnissen angemessen sind. ***Die Kommission sorgt für eine angemessene finanzielle Unterstützung im Regelungsrahmen bestehender Unionsprogramme, um insbesondere die Belastung von Kleinst-, Klein- und mittleren Unternehmen zu verringern.*** |

Oder. en

*Rechtfertigung*

*Es ist von entscheidender Bedeutung, dass die Kommission finanzielle Unterstützung bereitstellt, um die Einhaltung dieser Verordnung zu erleichtern, insbesondere für Kleinstunternehmen und KMU.*

**Abänderung 85**

**Vorschlag für eine Verordnung Artikel 24 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***Artikel 24a*** |
| | ***Vereinbarungen über die gegenseitige Anerkennung*** |
| | ***1. Zur Förderung des internationalen Handels bemüht sich die Kommission um den Abschluss von Abkommen über die gegenseitige Anerkennung (MRA) mit gleichgesinnten Drittländern. MRAs werden nur zwischen der Union und Drittländern geschlossen, die sich auf einem vergleichbaren technischen Entwicklungsstand befinden und ein kompatibles Konzept für die Konformitätsbewertung verfolgen. Sie müssen dasselbe Schutzniveau gewährleisten wie das in dieser Verordnung vorgesehene.*** |
| | ***2. Die Kommission bewertet internationale Normen und prüft, ob sie das gleiche Schutzniveau bieten wie die in dieser Verordnung vorgesehenen Normen, um die Entwicklung harmonisierter europäischer Normen zu*** |

***vereinfachen.***

Oder. en

**Abänderung 86**

**Vorschlag für eine Verordnung**
**Artikel 29 - Absatz 7 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(7a) Die Mitgliedstaaten und die Kommission ergreifen geeignete Maßnahmen, um sicherzustellen, dass ausreichend qualifizierte Fachkräfte zur Verfügung stehen, damit Engpässe bei der Tätigkeit der Konformitätsbewertungsstellen möglichst gering gehalten werden.*** |

Oder. en

**Abänderung 87**

**Vorschlag für eine**

**Verordnung**
**Artikel 29 - Absatz 12**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (12) Die Konformitätsbewertungsstellen arbeiten nach einheitlichen, fairen und angemessenen Bedingungen, wobei sie insbesondere die Interessen der ***KMU in Bezug auf*** die Gebühren berücksichtigen. | (12) Die Konformitätsbewertungsstellen arbeiten nach einheitlichen, fairen und angemessenen Bedingungen, wobei sie insbesondere die Interessen der ***Kleinstunternehmen sowie der kleinen und mittleren Unternehmen in Bezug auf*** die Gebühren berücksichtigen. |

Oder. en

**Abänderung 88**

**Vorschlag für eine**
**Verordnung Artikel 41 -**
**Absatz 6**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|

| | |
|---|---|
| 6. Die Mitgliedstaaten stellen sicher, dass die benannten Marktüberwachungsbehörden mit angemessenen finanziellen ***und personellen*** Ressourcen ausgestattet werden, damit sie ihre Aufgaben gemäß | 6. Die Mitgliedstaaten stellen sicher, dass die benannten Marktüberwachungsbehörden mit angemessenen finanziellen Mitteln ***und qualifiziertem Personal ausgestattet werden***, um folgende Aufgaben zu erfüllen |

ihre Aufgaben im Rahmen dieser Verordnung.

Oder. en

**Abänderung 89**

**Vorschlag für eine**

**Verordnung**
**Artikel 41 - Absatz 9 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(9a) Die Marktüberwachungsbehörden übermitteln der Kommission Daten über die von den Herstellern angegebene durchschnittliche erwartete Produktlebensdauer, aufgeschlüsselt nach Produktkategorien mit digitalen Elementen. Die Kommission veröffentlicht diese Informationen in einer öffentlich zugänglichen und benutzerfreundlichen Datenbank.*** |

Oder. en

**Abänderung 90**

**Vorschlag für eine**
**Verordnung Artikel 45 -**
**Absatz 1**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 1. Hat die Kommission hinreichende Gründe zu der Annahme, auch auf der Grundlage der von der ENISA vorgelegten Informationen, dass ein Produkt mit digitalen Elementen, das ein erhebliches Cybersicherheitsrisiko darstellt, die Anforderungen dieser Verordnung nicht erfüllt, ***kann*** sie die zuständigen Marktüberwachungsbehörden auffordern, eine Bewertung der Einhaltung der | Anforderungen vorzunehmen und die in Artikel 43 genannten Verfahren anzuwenden. |

1. Hat die Kommission hinreichende Gründe zu der Annahme, auch auf der Grundlage von Informationen der ENISA, dass ein Produkt mit digitalen Elementen, das ein erhebliches Cybersicherheitsrisiko darstellt, die Anforderungen dieser Verordnung nicht erfüllt**,** fordert sie die zuständigen Marktüberwachungsbehörden auf, eine Bewertung der Konformität vorzunehmen und die Verfahren nach Artikel 43 einzuhalten.

Oder. en

**Abänderung 91**

**Vorschlag für eine Verordnung Artikel 45 - Absatz 2**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 2. Unter außergewöhnlichen Umständen, die ein sofortiges Eingreifen zur Wahrung des ordnungsgemäßen Funktionierens des Binnenmarktes rechtfertigen, und wenn die Kommission hinreichende Gründe für die Annahme hat, dass das in Absatz 1 genannte Produkt die Anforderungen dieser Verordnung weiterhin nicht erfüllt und die zuständigen Marktüberwachungsbehörden keine wirksamen Maßnahmen ergriffen haben, ***kann*** die Kommission die ENISA auffordern, eine Bewertung der Konformität durchzuführen. Die Kommission unterrichtet die zuständigen Marktüberwachungsbehörden entsprechend. Die betroffenen Wirtschaftsakteure arbeiten soweit erforderlich mit der ENISA zusammen. | 2. (3) Unter außergewöhnlichen Umständen, die ein sofortiges Eingreifen zur Wahrung des ordnungsgemäßen Funktionierens des Binnenmarktes rechtfertigen, und wenn die Kommission hinreichende Gründe für die Annahme hat, dass das in Absatz 1 genannte Produkt die Anforderungen dieser Verordnung weiterhin nicht erfüllt und die zuständigen Marktüberwachungsbehörden keine wirksamen Maßnahmen ergriffen haben**,** fordert die Kommission die ENISA auf, eine Bewertung der Konformität vorzunehmen. Die Kommission unterrichtet die zuständigen Marktüberwachungsbehörden entsprechend. Die betroffenen Wirtschaftsakteure arbeiten soweit erforderlich mit der ENISA zusammen. |

Oder. en

**Abänderung 92**

**Vorschlag für eine Verordnung Artikel 48 - Absatz 1**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 1. Die Marktüberwachungsbehörden ***können mit anderen einschlägigen Behörden vereinbaren,*** gemeinsame Maßnahmen zur Gewährleistung der Cybersicherheit und des Verbraucherschutzes in Bezug auf bestimmte Produkte mit digitalen Elementen, die auf dem Markt in Verkehr gebracht oder bereitgestellt werden, durchzuführen, insbesondere bei | Produkten, bei denen häufig Cybersicherheitsrisiken festgestellt werden. |

| | | |
|---|---|---|
| 1. Marktüberwachungsbehörden führen gemeinsame Maßnahmen zur Gewährleistung der Cybersicherheit und des Verbraucherschutzes in Bezug auf bestimmte Produkte mit digitalen Elementen durch, die auf dem Markt in Verkehr gebracht oder bereitgestellt werden, insbesondere Produkte, bei denen häufig Cybersicherheitsrisiken festgestellt werden. | ***Die*** | |
| | Oder. en | |

**Abänderung 93**

**Vorschlag für eine Verordnung Artikel 48 - Absatz 2**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 2. Die Kommission oder die ENISA ***können*** gemeinsame Maßnahmen zur Überprüfung der Einhaltung dieser Verordnung vorschlagen, die von den Marktüberwachungsbehörden auf der Grundlage von Hinweisen oder Informationen über eine potenzielle, mehrere Mitgliedstaaten umfassende Nichtkonformität von Produkten, die in den Anwendungsbereich dieser Verordnung fallen, mit den in dieser Verordnung festgelegten Anforderungen durchzuführen sind. | 2. ***Die*** Kommission oder die ENISA schlagen gemeinsame Maßnahmen zur Überprüfung der Einhaltung dieser Verordnung vor, die von den Marktüberwachungsbehörden auf der Grundlage von Hinweisen oder Informationen über eine mögliche, mehrere Mitgliedstaaten betreffende Nichtkonformität von Produkten, die in den Anwendungsbereich dieser Verordnung fallen, mit den in dieser Verordnung festgelegten Anforderungen durchzuführen sind. |

Oder. en

**Abänderung 94**

**Vorschlag für eine Verordnung Artikel 49 - Absatz 1**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 1. Die Marktüberwachungsbehörden ***können beschließen,*** gleichzeitig koordinierte Kontrollmaßnahmen ("Sweeps") für bestimmte Produkte mit digitalen Elementen oder Produktkategorien durchzuführen, um die Einhaltung dieser Verordnung zu überprüfen oder um Verstöße gegen sie aufzudecken. | 1. Die Marktüberwachungsbehörden führen ***regelmäßig*** gleichzeitige koordinierte Kontrollaktionen ("Sweeps") für bestimmte Produkte mit digitalen Elementen oder Produktkategorien durch, um die Einhaltung dieser Verordnung zu überprüfen oder um Verstöße gegen diese Verordnung aufzudecken. ***Bei solchen Sweeps werden vorrangig Produkte mit digitalen Elementen überprüft, die von Herstellern in Verkehr gebracht werden, die ein Sicherheitsrisiko für die Union darstellen können. Sie umfassen Inspektionen von Produkten, die unter einer Tarnidentität erworben wurden, und zielen darauf ab, die Konformität*** |

***dieser Produkte mit dieser Verordnung zu überprüfen, insbesondere im Hinblick auf die Identifizierung potenzieller eingebetteter Hintertüren oder anderer ausnutzbarer Schwachstellen.***

Oder. en

*Rechtfertigung*

*Es ist wichtig, einen besonderen Schwerpunkt auf Hersteller zu legen, die ein Cyber-Sicherheitsrisiko für die Integrität der Union darstellen können.*

**Abänderung 95**

**Vorschlag für eine Verordnung Artikel 49 - Absatz 2**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 2. Sofern die beteiligten Marktaufsichtsbehörden nichts anderes vereinbaren, werden die Sweeps von der Kommission koordiniert. Der Koordinator des Sweeps ***kann gegebenenfalls*** die aggregierten Ergebnisse öffentlich zugänglich machen. | 2. Sofern die beteiligten Marktaufsichtsbehörden nichts anderes vereinbaren, werden die Sweeps von der Kommission koordiniert. ***Der*** Koordinator des Sweeps macht die aggregierten Ergebnisse öffentlich zugänglich. |

Oder. en

**Abänderung 96**

**Vorschlag für eine Verordnung Artikel 49 - Absatz 3**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 3. Die ENISA ***kann*** bei der Wahrnehmung ihrer Aufgaben, auch auf der Grundlage der gemäß Artikel 11 Absätze 1 und 2 eingegangenen Meldungen, Produktkategorien ermitteln, für die Sweeps organisiert werden ***können***. Der Vorschlag für Sweeps wird dem in Absatz 2 genannten potenziellen Koordinator zur Prüfung durch die Marktüberwachungsbehörden vorgelegt. | 3. ***Die*** ENISA ermittelt bei der Wahrnehmung ihrer Aufgaben, auch auf der Grundlage der gemäß Artikel 11 Absätze 1 und 2 eingegangenen Meldungen, die Produktkategorien, für die Sweeps durchgeführt werden ***sollen***. Der Vorschlag für Sweeps wird dem in Absatz 2 genannten potenziellen Koordinator zur Prüfung durch die Marktüberwachungsbehörden vorgelegt. |

Oder. en

**Abänderung 97**

**Vorschlag für eine Verordnung Artikel 49 - Absatz 5**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 5. Die Marktüberwachungsbehörden ***können*** Beamte der Kommission und andere von der Kommission ermächtigte Begleitpersonen zur Teilnahme an Sweeps einladen. | 5. ***Die*** Marktüberwachungsbehörden laden Beamte der Kommission und andere von der Kommission ermächtigte Begleitpersonen zur Teilnahme an Sweeps ein. |

Oder. en

**Abänderung 98**

**Vorschlag für eine Verordnung Artikel 50 - Absatz 2**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 2. Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 2 Absatz 4, Artikel 6 Absatz 2, Artikel 6 Absatz 3, Artikel 6 Absatz 5, Artikel ***20 Absatz 5 und*** Artikel 23 Absatz 5 wird der Kommission übertragen. | 2. Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 2 Absatz 4, Artikel 6 Absatz 2, Artikel 6 Absatz 3, Artikel 6 Absatz 5 und Artikel ***10 Absatz 15, Artikel 11 Absatz 5, Artikel 19 Absatz 1, Artikel 20 Absatz 5,*** Artikel 23 Absatz 5 ***und Artikel 53a*** werden der Kommission übertragen. |

Oder. en

**Abänderung 99**

**Vorschlag für eine Verordnung Artikel 50 - Absatz 3**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 3. Die in Artikel 2 Absatz 4, Artikel 6 Absatz 2 und Artikel 6 Absatz 3 genannte | Befugnisübertragung, Artikel 6 Absatz 5, Artikel ***20 Absatz 5 und*** Artikel 23 Absatz 5 können vom Europäischen |

| | |
|---|---|
| Parlament oder vom Rat jederzeit widerrufen werden. Ein Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss genannten Befugnis. Er wird an dem Tag wirksam, an dem | 3. Die in Artikel 2 Absatz 4, Artikel 6 Absatz 2 und Artikel 6 Absatz 3 genannte Befugnisübertragung,<br>Artikel 6 Absatz 5, Artikel ***10 Absatz 15, Artikel 11 Absatz 5,***<br>***Artikel 19 Absatz 1, Artikel 20 Absatz 5,***<br>Artikel 23 Absatz 5 ***und Artikel 53a***<br>können vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Ein Beschluss über den Widerruf beendet die Übertragung der Befugnis |

| | |
|---|---|
| nach der Veröffentlichung des Beschlusses im Amtsblatt der Europäischen Union oder zu einem im Beschluss genannten späteren Zeitpunkt. Die Gültigkeit bereits in Kraft getretener delegierter Rechtsakte wird davon nicht berührt. | die in dem Beschluss angegeben sind. Er wird am Tag nach der Veröffentlichung des Beschlusses im Amtsblatt der Europäischen Union oder zu einem darin angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit bereits in Kraft getretener delegierter Rechtsakte wird davon nicht berührt. |

Oder. en

**Abänderung 100**

**Vorschlag für eine Verordnung Artikel 50 - Absatz 6**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 6. Ein delegierter Rechtsakt, der gemäß Artikel 2 Absatz 4, Artikel 6 Absatz 2 oder Artikel 6 Absatz 3 erlassen wurde, Artikel 6 Absatz 5, Artikel ***20 Absatz 5 und*** Artikel 23 Absatz 5 treten nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung des betreffenden Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist sowohl das Europäische Parlament als auch der Rat der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Diese Frist wird auf Initiative des Europäischen Parlaments oder des Rates um zwei Monate verlängert. | 6. Ein delegierter Rechtsakt, der gemäß Artikel 2 Absatz 4, Artikel 6 Absatz 2 oder Artikel 6 Absatz 3 erlassen wurde, Artikel 6 Absatz 5, Artikel ***10 Absatz 15, Artikel 11 Absatz 5, Artikel 19 Absatz 1, Artikel 20 Absatz 5,*** Artikel 23 Absatz 5 ***und Artikel 53a*** treten nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erheben oder wenn vor Ablauf dieser Frist sowohl das Europäische Parlament als auch der Rat der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Diese Frist wird auf Initiative des Europäischen Parlaments oder des Rates um zwei Monate verlängert. |

Oder. en

**Abänderung 101**

**Vorschlag für eine Verordnung Artikel 53 -**

**Absatz 1**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
| --- | --- |
| 1. Die Mitgliedstaaten legen die Sanktionen fest, die bei Verstößen von Wirtschaftsteilnehmern gegen | 1. Die Mitgliedstaaten legen die Sanktionen fest, die bei Verstößen von Wirtschaftsteilnehmern gegen |

| | |
|---|---|
| und ergreifen alle erforderlichen Maßnahmen, um ihre Durchsetzung zu gewährleisten. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. | und ergreifen alle erforderlichen Maßnahmen, um ihre Durchsetzung zu gewährleisten. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein***. Sie stellen sicher, dass diese Vorschriften den finanziellen Möglichkeiten von Kleinst-, kleinen und mittleren Unternehmen Rechnung tragen***. |

Oder. en

**Abänderung 102**

**Vorschlag für eine Verordnung Artikel 53 - Absatz 2**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 2. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen unverzüglich mit und unterrichten sie unverzüglich über alle späteren Änderungen. | 2. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen unverzüglich mit und unterrichten sie unverzüglich über alle späteren Änderungen, die sie betreffen. ***Die Kommission stellt sicher, dass diese Vorschriften und Maßnahmen in der gesamten Union einheitlich und kohärent angewandt werden.*** |

Oder. en

**Abänderung 103**

**Vorschlag für eine Verordnung Artikel 53 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***Artikel 53a*** |
| | ***Zuweisung der Einnahmen aus den Sanktionen zur Förderung der Cybersicherheit in der Europäischen Union*** |

***1. Die Einnahmen aus den in Artikel 53 Absatz 1 genannten Sanktionen werden für Projekte zur Verbesserung der Cybersicherheit in der Union verwendet. Diese***

***Die Projekte haben folgende Ziele:***

***(i) die Zahl der qualifizierten Fachkräfte im Bereich der Cybersicherheit zu erhöhen;***

***(ii) den Aufbau von Kapazitäten für Kleinst-, Klein- und mittlere Unternehmen zu fördern, damit sie diese Verordnung besser einhalten können;***

***(iii) Verbesserung des kollektiven Situationsbewusstseins in Bezug auf Cyber-Bedrohungen;***

***(iv) Entwicklung von Instrumenten zur Verbesserung der Widerstandsfähigkeit von Unionsunternehmen gegenüber dem Diebstahl von geistigem Eigentum über das Internet.***

***2. Die in Absatz 1 genannten Einnahmen werden dem Programm "Digitales Europa" gemäß Artikel 6 der Verordnung (EU) 2021/694 zugewiesen. Sie sind für die Verbesserung der Cybersicherheit in der Union bestimmt. Es handelt sich um zweckgebundene Einnahmen im Sinne von Artikel 21 Absatz 5 der Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates[1], die gemäß den für das Programm "Digitales Europa" geltenden Vorschriften ausgeführt werden. Sie gelten als Aufstockung des Haushalts und dürfen nicht zur Verringerung des Beitrags aus dem Unionshaushalt verwendet werden.***

***3. Die Kommission wird ermächtigt, delegierte Rechtsakte gemäß Artikel 50 zu erlassen, um diese Verordnung hinsichtlich der Modalitäten für die Zahlung der in Artikel 53 genannten Sanktionen zu ergänzen.***

---

***[1] Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates vom 18. Juli 2018 über die Finanzvorschriften für den***

***Gesamthaushaltsplan der Union und zur Änderung der Verordnungen (EU) Nr. 1296/2013, (EU) Nr. 1301/2013, (EU) Nr. 1303/2013, (EU) Nr. 1304/2013, (EU) Nr. 1309/2013, (EU) Nr. 1316/2013, (EU) Nr. 223/2014, (EU) Nr. 283/2014, und des Beschlusses Nr. 541/2014/EU und zur Aufhebung der Verordnung (EU, Euratom)***

***Nr. 966/2012 (ABl. L 193 vom 30.7.2018, S. 1).***

Oder. en

**Abänderung 104**

**Vorschlag für eine**

**Verordnung**
**Artikel 55 - Absatz 3 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(3a) Bis zum ... [40 Monate nach dem Inkrafttreten dieser Verordnung] können die Hersteller die Anforderungen dieser Verordnung auf freiwilliger Basis erfüllen. Wenn Hersteller diese Verordnung in Bezug auf ihre Produkte mit digitalen Elementen einhalten, wird davon ausgegangen, dass sie auch die Delegierte Verordnung (EU) 2022/30 einhalten.*** |
| | ***Nach ... [40 Monate nach dem Inkrafttreten dieser Verordnung hebt die Kommission die Delegierte Verordnung (EU) 2022/30 der Kommission auf.*** |

Oder. en

*Rechtfertigung*

*Um die frühzeitige Einhaltung der CRA zu fördern, sollte eine Vermutung der Konformität mit der delegierten Verordnung gemäß der Funkanlagenrichtlinie gewährt werden.*

**Abänderung 105**

**Vorschlag für eine**

**Verordnung**
**Artikel 56 - Absatz 1 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***Die Kommission legt jedes Jahr bei der Vorlage des Haushaltsentwurfs für das*** |

***folgende Jahr eine detaillierte Bewertung der Aufgaben der ENISA im Rahmen dieser Verordnung gemäß Anhang VIa und anderer einschlägiger Rechtsvorschriften der Union vor und erläutert im Einzelnen***

| | |
|---|---|
| | ***die zur Erfüllung dieser Aufgaben erforderlichen finanziellen und personellen Ressourcen.*** |

Oder. en

**Abänderung 106**

**Vorschlag für eine Verordnung Artikel 57 - Absatz 2**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| Er gilt ab dem [***24*** Monate nach dem Inkrafttreten dieser Verordnung]. Artikel 11 gilt jedoch ab dem [***12*** Monate nach dem Inkrafttreten dieser Verordnung]. | Sie gilt ab ... [***40*** Monate nach Inkrafttreten dieser Verordnung]. Artikel 11 gilt jedoch ab dem [***20*** Monate nach dem Inkrafttreten dieser Verordnung]. |

Oder. en

*Rechtfertigung*

*Angesichts des horizontalen Charakters, des breiten Anwendungsbereichs und der Komplexität dieser Verordnung sollte den Wirtschaftsbeteiligten ausreichend Zeit zur Anpassung an diese Verordnung eingeräumt werden.*

**Abänderung 107**

**Vorschlag für eine Verordnung Anhang I - Teil 1 - Nummer 2**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| ***(2) Produkte mit digitalen Elementen müssen ohne bekannte ausnutzbare Schwachstellen geliefert werden;*** | ***gelöscht*** |

Oder. en

*Begründung*

*Verschoben unter Punkt (3) - auf der Grundlage der*

*Risikobewertung*

**Abänderung 108**

**Vorschlag für eine Verordnung**
**Anhang I - Teil 1 - Nummer 3 - Buchstabe -a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***(-a)ohne bekannte ausnutzbare Schwachstellen ausgeliefert werden;*** |

Oder. en

*Rechtfertigung*

*Da einige Schwachstellen ein sehr geringes oder gar kein Cybersicherheitsrisiko darstellen können, sollte die Verpflichtung zur Lieferung von Produkten ohne bekannte ausnutzbare Schwachstellen risikobasiert sein.*

**Abänderung 109**

**Vorschlag für eine**

**Verordnung**
**Anhang I - Teil 1 - Nummer 3 - Buchstabe a**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (a) mit einer sicheren Standardkonfiguration geliefert werden, einschließlich der Möglichkeit, das Produkt in seinen ursprünglichen Zustand zurückzusetzen; | (a) mit einer sicheren Standardkonfiguration ausgeliefert werden, einschließlich der Möglichkeit, das Produkt in seinen ursprünglichen Zustand zurückzusetzen***, wobei alle Sicherheitsaktualisierungen erhalten bleiben***; |

Oder. en

**Abänderung 110**

**Vorschlag für eine**

**Verordnung**
**Anhang I - Teil 2 - Absatz 1 - Nummer 2**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|

| | |
|---|---|
| (2) in Bezug auf die Risiken, die mit den Produkten mit digitalen Elementen verbunden sind, Schwachstellen unverzüglich zu beseitigen, auch durch die Bereitstellung von Sicherheitsupdates; | (2) in Bezug auf die Risiken, die mit den Produkten mit digitalen Elementen verbunden sind, Schwachstellen unverzüglich zu beheben, unter anderem durch die Bereitstellung von Sicherheitsupdates***, die gegebenenfalls automatisch installiert werden***; |

Oder. en

**Abänderung 111**

**Vorschlag für eine**

**Verordnung**
**Anhang II - Absatz 1 - Nummer 8**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 8. die Art der technischen Sicherheitsunterstützung, die der Hersteller anbietet, und bis wann sie geleistet wird, zumindest bis zu dem Zeitpunkt, zu dem die Nutzer mit Sicherheitsaktualisierungen rechnen können; | 8. ***die voraussichtliche Lebensdauer des Produkts,*** die Art der vom Hersteller angebotenen technischen Sicherheitsunterstützung und den Zeitpunkt, bis zu dem sie geleistet wird, zumindest aber den Zeitpunkt, bis zu dem die Nutzer mit Sicherheitsaktualisierungen rechnen können, ***sowie, sofern möglich und zutreffend, eine Mitteilung über das Ende der Sicherheitsaktualisierungen***; |

Oder. en

**Abänderung 112**

**Vorschlag für eine**

**Verordnung**
**Anhang III - Teil I - Nummer 18**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| ***Router, Modems für den Anschluss an das Internet und Switches, die nicht unter die Klasse II fallen;*** | ***gelöscht*** |

*Rechtfertigung*

*Vollständig in Klasse II überführt - Router und Modems sind der Schlüssel zur Cybersicherheit*

**A**

**b**

**ä**

**n**

**d**

**erung 113 Vorschlag für**

**eine Verordnung**
**Anhang III - Teil I - Nummer 22**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 22. industrielle Automatisierungs- und Steuerungssysteme (InVeKoS), die nicht unter die Klasse II fallen, wie z. B. speicherprogrammierbare Steuerungen (SPS), verteilte Steuerungssysteme (DCS), rechnergestützte numerische Steuerungen für Werkzeugmaschinen (CNC) und übergeordnete Steuerungs- und Datenerfassungssysteme (SCADA); | 22. industrielle Automatisierungs- und Steuerungssysteme (Industrial Automation & Control Systems, IACS), die nicht unter die Klasse II fallen, wie z. B. speicherprogrammierbare Steuerungen (PLC), verteilte Steuerungssysteme (DCS), rechnergestützte numerische Steuerungen für Werkzeugmaschinen (CNC)***, Industrieroboter und ihre Steuerungssysteme, mobile Maschinen*** und überwachte Steuerungs- und Datenerfassungssysteme (SCADA); |

Oder. en

**Abänderung 114**

**Vorschlag für eine**

**Verordnung**
**Anhang III - Teil I - Nummer 23 a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***23a.Hausautomatisierungssysteme;*** |

Oder. en

*Rechtfertigung*

*Hausautomatisierungssysteme spielen eine Schlüsselrolle in den Häusern der Bürger und sollten daher als kritische Produkte betrachtet werden.*

**Abänderung 115**

**Vorschlag für eine**

**Verordnung**
**Anhang III - Teil I - Nummer 23 b (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| | ***23b. Private Sicherheitsvorkehrungen.*** |

Oder. en

*Rechtfertigung*

*Sicherheitskameras oder intelligente Schlösser sind für die Sicherheit der Bürger unerlässlich und sollten daher*

*die als kritische Produkte gelten.*

**Abänderung 116**

**Vorschlag für eine**

**Verordnung**
**Anhang III - Teil II - Nummer 7**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 7. die Router, die Modems für den Anschluss an das Internet und die Switches***, die für den industriellen Einsatz*** bestimmt sind; | 7. die Router, die Modems für den Anschluss an das Internet und die Switches; |

Oder. en

**Abänderung 117**

**Vorschlag für eine**

**Verordnung**
**Anhang III - Teil II - Nummer 14**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| ***14. sensorische und aktorische Komponenten von Robotern und Robotersteuerungen;*** | ***gelöscht*** |

Oder. en

**Abänderung 118**

**Vorschlag für eine**

**Verordnung**
**Anhang VI - Teil A - Nummer 4 - Nummer 4.2**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 4.2 Der Hersteller stellt für jedes Produkt mit digitalen Elementen eine schriftliche EU-Konformitätserklärung | gemäß Artikel 20 aus und hält sie zusammen mit den technischen Unterlagen nach dem Inverkehrbringen des Produkts mit digitalen |

| | |
|---|---|
| Elementen zehn Jahre lang für die nationalen Behörden bereit. In der EU-Konformitätserklärung wird das Produkt mit digitalen Elementen gekennzeichnet | 4.2 Der Hersteller stellt für jedes Produkt mit digitalen Elementen eine schriftliche EU-Konformitätserklärung gemäß Artikel 20 aus und hält sie zusammen mit den technischen Unterlagen zehn Jahre lang nach dem Inverkehrbringen des Produkts mit digitalen Elementen ***oder über die voraussichtliche Lebensdauer des Produkts, je nachdem, welcher Zeitraum länger ist, für die*** nationalen Behörden bereit. Die EU-Erklärung über |

für die sie ausgestellt worden ist. Eine Kopie der EU-Konformitätserklärung wird den zuständigen Behörden auf Anfrage zur Verfügung gestellt.

Konformitätserklärung muss das Produkt mit den digitalen Elementen identifizieren, für das sie ausgestellt wurde. Eine Kopie der EU-Konformitätserklärung wird den zuständigen Behörden auf Verlangen zur Verfügung gestellt.

Oder. en

**Abänderung 119**

**Vorschlag für eine**

**Verordnung**
**Anhang VI - Teil B - Nummer 9**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (9) Der Hersteller hält ein Exemplar der EU-Baumusterprüfbescheinigung, ihrer Anhänge und Ergänzungen zusammen mit den technischen Unterlagen zehn Jahre lang nach Inverkehrbringen des Produkts für die nationalen Behörden bereit. | (9) Der Hersteller hält ein Exemplar der EU-Baumusterprüfbescheinigung, ihrer Anhänge und Ergänzungen zusammen mit den technischen Unterlagen zehn Jahre lang nach dem Inverkehrbringen des Produkts ***oder während der voraussichtlichen Lebensdauer des Produkts, je nachdem, welcher Zeitraum länger ist, für die*** nationalen Behörden bereit. |

Oder. en

**Abänderung 120**

**Vorschlag für eine**

**Verordnung**
**Anhang VI - Teil C - Nummer 3 - Nummer 3.2**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| 3.2 Der Hersteller stellt für ein Produktmodell eine schriftliche Konformitätserklärung aus und hält sie zehn Jahre lang nach dem Inverkehrbringen des Produkts für die nationalen Behörden bereit. In der | Konformitätserklärung ist das Produktmodell anzugeben, für das sie ausgestellt wurde. Eine Kopie der Konformitätserklärung wird den zuständigen Behörden auf Verlangen zur Verfügung gestellt. |

3.2 Der Hersteller stellt für ein Produktmodell eine schriftliche Konformitätserklärung aus und hält sie zehn Jahre lang nach dem Inverkehrbringen des Produkts ***oder, falls dieser Zeitraum länger ist, während der voraussichtlichen Lebensdauer des Produkts für*** die nationalen Behörden bereit. In der Konformitätserklärung ist das Produktmodell anzugeben, für das sie ausgestellt wurde. Eine Kopie der Konformitätserklärung wird den zuständigen Behörden auf Verlangen zur Verfügung gestellt.

Oder. en

**Abänderung 121**

**Vorschlag für eine**

**Verordnung**
**Anhang VI - Teil H - Nummer 5 - Nummer 5.2 - Absatz 1**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| Der Hersteller stellt für jedes Produktmodell eine schriftliche Konformitätserklärung aus und hält sie zehn Jahre lang nach dem Inverkehrbringen des Produkts für die nationalen Behörden bereit. In der Konformitätserklärung ist das Produktmodell anzugeben, für das sie ausgestellt wurde. | Der Hersteller stellt für jedes Produktmodell eine schriftliche Konformitätserklärung aus und hält sie zehn Jahre lang nach dem Inverkehrbringen des Produkts ***oder während der voraussichtlichen Lebensdauer des Produkts, je nachdem, welcher Zeitraum länger ist, für die*** nationalen Behörden bereit. In der Konformitätserklärung ist das Produktmodell anzugeben, für das sie ausgestellt wurde. |

Oder. en

**Abänderung 122**

**Vorschlag für eine**

**Verordnung**
**Anhang VI - Teil H - Nummer 6 - einleitender Teil**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
|---|---|
| (6) Der Hersteller hält für einen Zeitraum von mindestens zehn Jahren nach dem Inverkehrbringen des Produkts für die nationalen Behörden Unterlagen bereit: | (6) Der Hersteller hält während eines Zeitraums von mindestens zehn Jahren nach dem Inverkehrbringen des Produkts ***oder während der voraussichtlichen Lebensdauer des Produkts, je nachdem, welcher Zeitraum länger ist, die Unterlagen für die*** nationalen Behörden zur Verfügung: |

Oder. en

**Abänderung 123**

**Vorschlag für eine Verordnung Anhang VI a (neu)**

| *Von der Kommission vorgeschlagener Text* | *Abänderung* |
| --- | --- |
| | ***Kapazitätsbedarf der Agentur der Europäischen Union für Cybersicherheit (ENISA)*** |
| | ***Damit die ENISA ihren Verpflichtungen im Rahmen dieser Verordnung nachkommen kann und um die bestehenden Verpflichtungen der Agentur im Rahmen anderer Rechtsvorschriften der Union nicht zu gefährden, ist eine angemessene Personal- und Finanzausstattung der ENISA sicherzustellen. Daher werden zusätzliche Aufgaben der ENISA im Rahmen dieser Verordnung mit zusätzlichen personellen und finanziellen Ressourcen verbunden. 8,5 zusätzliche Vollzeitstellen und entsprechende zusätzliche Mittel werden benötigt, um die zusätzlichen Aufgaben im Rahmen dieser Verordnung zu erfüllen.*** |
| | Oder. en |

## BEGRÜNDUNG

Die Berichterstatterin begrüßt nachdrücklich den Vorschlag der Kommission zur Behebung von Cybersicherheitsmängeln bei Hardware- und Softwareprodukten. Im Jahr 2021 werden sich die weltweiten Kosten der Cyberkriminalität auf schwindelerregende 5,5 Billionen Euro belaufen. Dieses Phänomen in Verbindung mit der zunehmenden Digitalisierung fordert die Gesetzgeber auf, dafür zu sorgen, dass geeignete Cybersicherheitsmaßnahmen vorhanden sind, um die Interessen der Verbraucher und der Industrie zu schützen.

In diesem Zusammenhang begrüßt der Berichterstatter, dass die Kommission einen ehrgeizigen Vorschlag vorgelegt hat, der das allgemeine Niveau der Cybersicherheit in den Mitgliedstaaten und das Funktionieren des Binnenmarktes verbessern wird. Ein harmonisierter Rechtsrahmen ist notwendig, damit Unternehmen, die im Binnenmarkt tätig sind, von Rechtsklarheit profitieren können, und um sicherzustellen, dass die Union eine führende Rolle bei der Festlegung von Normen für die Cybersicherheit auf der globalen Bühne spielen kann.

Was den Anwendungsbereich betrifft, so stimmt der Berichterstatter dem Vorschlag der Kommission zu, alle Produkte mit digitalen Elementen einzubeziehen. Dieser umfassende Ansatz würde die Einhaltung der Cybersicherheit in der gesamten Wertschöpfungskette gewährleisten und die Wettbewerbsfähigkeit und Attraktivität von in der Union hergestellten Produkten verbessern. Es ist jedoch notwendig, den derzeitigen Wortlaut zu vereinfachen und sich auf direkt und indirekt anschließbare Produkte zu beziehen, während Ersatzteile, die ausschließlich für den Reparaturprozess bestimmt sind und bereits vor der Umsetzung dieser Verordnung auf dem Markt waren, ausgeschlossen werden. In Bezug auf Open-Source-Software ist sich der Berichterstatter der Notwendigkeit bewusst, diese wichtige Innovationsquelle zu schützen, und hat daher eine Änderung vorgeschlagen, um sicherzustellen, dass von den Entwicklern nicht erwartet werden sollte, dass sie diese Verordnung einhalten, wenn sie keine finanzielle Gegenleistung für ihre Projekte erhalten. Nichtsdestotrotz sollte Open-Source-Software, die im Rahmen einer kommerziellen Tätigkeit bereitgestellt wird, abgedeckt sein, um die Cybersicherheit des Ökosystems der Union zu gewährleisten.

Während die überwiegende Mehrheit der Produkte mit digitalen Elementen nur einer Selbstbewertung unterzogen werden muss, werden kritische Produkte gemäß Artikel 6 einer Bewertung durch Dritte unterzogen. In dieser Frage ist der Berichterstatter der Ansicht, dass die Verordnung verbessert werden sollte, indem mehr Klarheit darüber geschaffen wird, wie oft die Liste in Anhang III geändert werden kann und welche Verfahren zu befolgen sind, nachdem ein Produkt in diese Liste aufgenommen wurde. Letzteres ist besonders wichtig, um den Unternehmen ausreichend Zeit für die Anpassung zu geben. Die Berichterstatterin ist jedoch der Ansicht, dass Hausautomatisierungssysteme und Produkte, die die private Sicherheit erhöhen, wie Kameras und intelligente Schlösser, als kritische Produkte der Klasse I eingestuft werden sollten, da die Unversehrtheit dieser Waren für die Sicherheit und die Privatsphäre der Bürger von größter Bedeutung ist.

Darüber hinaus sieht der Berichtsentwurf eine stärkere Beteiligung der Interessengruppen durch die Einrichtung einer Expertengruppe für Cyber-Resilienz vor. Dieses Gremium sollte damit beauftragt werden, die Kommission zu beraten und eine aktive Rolle bei der Ausarbeitung der in dieser Verordnung genannten delegierten Rechtsakte zu übernehmen.

Um die Interessen aller Seiten umfassend zum Ausdruck zu bringen, sollte sich die Expertengruppe aus Institutionen, der Industrie, der Zivilgesellschaft, der Wissenschaft und einzelnen Experten zusammensetzen.

Zusätzlich zu dem oben genannten Thema betont der Berichtsentwurf die Notwendigkeit für die Mitgliedstaaten, bei der öffentlichen Beschaffung von Produkten mit digitalen Elementen die Cybersicherheit stark zu berücksichtigen und sicherzustellen, dass Schwachstellen umgehend behoben werden.
Was die Verpflichtungen der Hersteller betrifft, so ist der Berichterstatter der Ansicht, dass ein fester Termin für die

die erwartete Produktlebensdauer ist für eine horizontale Verordnung, die eine breite Palette von Produkten von Software über Telefone bis hin zu Industriemaschinen abdecken soll, unzureichend. Aus diesem Grund hält es die Berichterstatterin für angemessener, die Hersteller die Lebensdauer ihrer jeweiligen Produkte bestimmen zu lassen, sofern die vorgeschlagene Dauer mit den vernünftigen Erwartungen der Verbraucher vereinbar ist. Eine flexible Dauer würde es den Herstellern auch ermöglichen, ihre Produkte zu präsentieren und eine lange Lebensdauer als Element der Wettbewerbsfähigkeit zu haben. Um die Verbraucher für dieses Thema zu sensibilisieren, sollte die Verordnung die Hersteller verpflichten, die voraussichtliche Produktlebensdauer deutlich auf der Verpackung anzugeben oder in die vertraglichen Vereinbarungen aufzunehmen und die Verbraucher über das bevorstehende Ende der Lebensdauer zu informieren. Darüber hinaus will der Berichtsentwurf den Schwerpunkt auf die Sicherheit legen. Daher ist der Berichterstatter der Ansicht, dass die Hersteller auch verpflichtet werden sollten, die Sicherheitsmerkmale ihres jeweiligen Produkts automatisch zu aktualisieren, wenn dies möglich ist. Wenn ein Hersteller eine voraussichtliche Lebensdauer von weniger als fünf Jahren festgelegt hat, sollte er bereit sein, vertragliche Vereinbarungen mit Unternehmen zu treffen, die Dienstleistungen erbringen wollen, die die Lebensdauer eines Produkts verlängern, und ihnen seinen Quellcode offen zu legen. Diese Möglichkeit sollte nicht zu einer Übertragung des Eigentums oder zur Offenlegung des Quellcodes führen.

Was die Meldepflichten gemäß Artikel 11 betrifft, so möchte der Berichterstatter den Zeitplan an die NIS2 anpassen, um mehr Kohärenz und Rechtssicherheit für die Beteiligten zu schaffen. In diesem Sinne schlägt der Berichterstatter vor, signifikante Vorfälle (und nicht alle Vorfälle) sowie aktiv ausgenutzte Sicherheitslücken zu melden, sofern klare Protokolle über den sicheren Umgang mit solchen Meldungen vorhanden sind, um die Verbreitung von Informationen über nicht gepatchte Sicherheitslücken zu vermeiden. Der Berichterstatter führt auch einen Mechanismus für die freiwillige Meldung von anderen Vorfällen, Beinaheunfällen und Cyberbedrohungen ein.

Um die Wirkung der Berichterstattung zu maximieren, ist es jedoch wichtig, eine einzige Anlaufstelle zu haben, auch um die Meldepflichten für die Hersteller in der gesamten Union zu vereinfachen. In diesem Zusammenhang ist der Berichterstatter der Ansicht, dass die ENISA die beste Institution für diese Aufgabe ist. Daher sollte die Kommission in Anbetracht der Erweiterung der Aufgaben und Zuständigkeiten der ENISA den Finanzbogen zu dieser Verordnung dahingehend ändern, dass die Agentur der Europäischen Union für Cybersicherheit mit zusätzlichen Stellen und entsprechenden zusätzlichen Mitteln ausgestattet wird, um die in dieser Verordnung festgelegten zusätzlichen Aufgaben der Agentur zu erfüllen.

Darüber hinaus ist es für den Berichterstatter von grundlegender Bedeutung, sicherzustellen, dass die Unternehmen bei der Umsetzung der Anforderungen dieser Verordnung ausreichend unterstützt werden. Dies gilt insbesondere für Kleinst-, kleine und mittlere Unternehmen, für die es angesichts ihrer begrenzten Möglichkeiten schwierig sein kann, die Einhaltung der Ratingagentur zu gewährleisten. Daher hält es die Berichterstatterin für unerlässlich, den Zeitpunkt, ab dem die Verordnung gilt, auf 40 Monate zu verlängern. In dieser Übergangszeit sollte es den Herstellern möglich sein, die CRA auf freiwilliger Basis einzuhalten, um eine Konformitätsvermutung mit der delegierten Verordnung zur Funkanlagenrichtlinie zu erhalten und sich an diese Verordnung anzupassen, bevor sie offiziell in Kraft tritt. Darüber hinaus möchte der Berichterstatter betonen, wie wichtig es für die Union ist, die Aus- und Weiterbildung von Arbeitnehmern zu unterstützen und die

Verfügbarkeit von Fachkräften für Cybersicherheit zu gewährleisten - ein Schlüsselelement für den Erfolg dieser Verordnung.

Darüber hinaus fordert die Berichterstatterin als allgemeinen Ansatz zur Unterstützung aller Beteiligten Leitlinien der Kommission, um die tatsächliche Umsetzungsphase genauer zu spezifizieren und so mehr Klarheit für alle Beteiligten zu schaffen.

Eine weitere, ebenso dringende Angelegenheit für den Berichterstatter ist der internationale Handel. Deshalb fordert der Berichtsentwurf die Kommission auf, Abkommen über die gegenseitige Anerkennung mit gleichgesinnten Drittländern in Erwägung zu ziehen, wenn diese einen vergleichbaren technischen Entwicklungsstand aufweisen und einen kompatiblen Ansatz bei der Konformitätsbewertung verfolgen, der das gleiche Schutzniveau gewährleistet wie das in dieser Verordnung vorgesehene. Dennoch ist es von wesentlicher Bedeutung, dass eine angemessene Überwachung von Produkten aus Risikoländern, die Hintertüren oder andere Schwachstellen enthalten können, gewährleistet ist: Die ENISA sollte sich mit den Marktaufsichtsbehörden abstimmen und die erforderlichen Kontrollen bei Anbietern durchführen, die ein höheres Risikoprofil aufweisen könnten.

Schließlich ist der Berichterstatter der Ansicht, dass die Einnahmen aus den Sanktionen für Projekte verwendet werden sollten, die das allgemeine Cybersicherheitsniveau in der Union anheben, und daher dem Programm "Digitales Europa" zugewiesen werden sollten, um Projekte zu unterstützen, die u. a. auf die Umschulung und Höherqualifizierung der derzeitigen Arbeitskräfte abzielen.

## ANHANG: LISTE DER EINRICHTUNGEN ODER PERSONEN VON DENEN DER BERICHTERSTATTER BEITRÄGE ERHALTEN HAT

| Körperschaft und/oder Person |
|---|
| (ISC)2 |
| ACEM |
| Fluggesellschaften4Europe |
| Allianz für IoT- und Edge-Computing-Innovationen |
| Amazon |
| Amerikanische Handelskammer |
| ANEC |
| Apfel |
| APPLiA |
| Associazione Italiana Internet-Anbieter |
| BDI |
| Beuc |
| Bitkom |
| BritCham |
| Broadcom |
| BSA - Die Software-Allianz |
| Business Europa |
| Kartenzahlung Schweden |
| CEMA |
| Centrum für Europäische Politik |
| CNH |
| Verband der dänischen Industrie (DI) |
| Confindustria |
| Cybersecurity-Koalition |
| DEKRA |
| Deutsche Telekom |
| Allianz der Entwickler |
| Digitales Europa |
| Enedis |
| Technik |
| Ericsson |
| ESMIG |
| ETNO |
| ETRMA |
| Europäische Organisation für Cybersicherheit |
| Europäischer Verband für Materialtransport (FEM) |
| Eurosmart |
| Federunacoma |
| Stiftung Freie Software Europa |
| Gesamtverband der Deutschen Versicherungswirtschaft |
| Giesecke+Devrient |
| GitHub |

| |
|---|
| Google |
| GSMA |
| Hanbury-Strategie |
| Huawei |
| IBM |
| Unabhängiger Einzelhandel Europa |
| Rat der Informationstechnologie-Industrie |
| Leaseurope |
| Lenovo |
| Verband der Maschinenindustrie (VDMA) |
| MedTechEurope |
| Microsoft |
| Okta |
| Offenes Forum Europa |
| Orange |
| Orgalim |
| Ständige Vertretung von Belgien |
| Ständige Vertretung von Italien |
| Ständige Vertretung der Niederlande |
| Piaggio |
| Datenschutz International |
| SAP |
| Schneider Elektrisch |
| Siemens |
| SME United |
| Splunk |
| Technologie-Industrie in Finnland |
| Telefonica |
| TIC-Rat |
| Trellix |
| Twillio |
| Unife |
| Vodafone-Gruppe |
| Wikimedia |
| Worldr |
| Xiaomi |
| Vergrößern |