Europäisches Parlament
2019-2024

Plenarsitzungsdokument

A9-0313/2021

4.11.2021

***I
BERICHT

über den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Ausschuss für Industrie, Forschung und Energie

Berichterstatter: Bart Groothuis

Verfasser der Stellungnahme (*):
Lukas Mandl, Ausschuss für bürgerliche Freiheiten, Justiz und Inneres

(*) Assoziierte Ausschüsse – Artikel 57 der Geschäftsordnung

Erklärung der benutzten Zeichen

*	Anhörungsverfahren
***	Zustimmungsverfahren
***I	Ordentliches Gesetzgebungsverfahren (erste Lesung)
***II	Ordentliches Gesetzgebungsverfahren (zweite Lesung)
***III	Ordentliches Gesetzgebungsverfahren (dritte Lesung)

(Die Angabe des Verfahrens beruht auf der im Entwurf eines Rechtsakts vorgeschlagenen Rechtsgrundlage.)

Änderungsanträge zu einem Entwurf eines Rechtsakts

Änderungsanträge des Parlaments in Spaltenform

Streichungen werden durch ***Fett- und Kursivdruck*** in der linken Spalte gekennzeichnet. Textänderungen werden durch ***Fett- und Kursivdruck*** in beiden Spalten gekennzeichnet. Neuer Text wird durch ***Fett- und Kursivdruck*** in der rechten Spalte gekennzeichnet.

Aus der ersten und der zweiten Zeile des Kopftextes zu jedem der Änderungsanträge ist der betroffene Abschnitt des zu prüfenden Entwurfs eines Rechtsakts ersichtlich. Wenn sich ein Änderungsantrag auf einen bestehenden Rechtsakt bezieht, der durch den Entwurf eines Rechtsakts geändert werden soll, umfasst der Kopftext auch eine dritte und eine vierte Zeile, in der der bestehende Rechtsakt bzw. die von der Änderung betroffene Bestimmung des bestehenden Rechtsakts angegeben werden.

Änderungsanträge des Parlaments in Form eines konsolidierten Textes

Neue Textteile sind durch ***Fett- und Kursivdruck*** gekennzeichnet. Auf Textteile, die entfallen, wird mit dem Symbol ▌ hingewiesen oder diese Textteile erscheinen durchgestrichen. Textänderungen werden gekennzeichnet, indem der neue Text in ***Fett- und Kursivdruck*** steht und der bisherige Text gelöscht oder durchgestrichen wird.
Rein technische Änderungen, die von den Dienststellen im Hinblick auf die Erstellung des endgültigen Textes vorgenommen werden, werden allerdings nicht gekennzeichnet.

INHALT

Seite

ENTWURF EINER LEGISLATIVEN ENTSCHLIESSUNG DES EUROPÄISCHEN PARLAMENTS

zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

(Ordentliches Gesetzgebungsverfahren: erste Lesung)

Das Europäische Parlament,

– unter Hinweis auf den Vorschlag der Kommission an das Europäische Parlament und den Rat (COM(2020)0823),

– 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 (C9-0422/2020),

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

– unter Hinweis auf die Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses vom 27. April 2021[1],

– nach Anhörung des Ausschusses der Regionen,

– gestützt auf Artikel 59 seiner Geschäftsordnung,

– unter Hinweis auf die Stellungnahmen des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres, des Ausschusses für auswärtige Angelegenheiten, des Ausschusses für Binnenmarkt und Verbraucherschutz sowie des Ausschusses für Verkehr und Tourismus,

– unter Hinweis auf den Bericht des Ausschusses für Industrie, Forschung und Energie (A9-0313/2021),

1. legt den folgenden Standpunkt in erster Lesung fest;

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

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

[1] ABl. C 286 vom 16.7.2021, S. 170.

Änderungsantrag 1

Vorschlag für eine Richtlinie
Titel

Vorschlag der Kommission	*Geänderter Text*
Vorschlag für eine	Vorschlag für eine
RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES	RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES
über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148	über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union ***(NIS-2-Richtlinie)*** und zur Aufhebung der Richtlinie (EU) 2016/1148

Änderungsantrag 2

Vorschlag für eine Richtlinie
Erwägung 1

Vorschlag der Kommission	*Geänderter Text*
(1) Ziel der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates[11] war der unionsweite Aufbau von Cybersicherheitskapazitäten, die Eindämmung von Bedrohungen für Netz- und Informationssysteme, die zur Erbringung wesentlicher Dienste in Schlüsselsektoren verwendet werden, und die Sicherstellung der Kontinuität solcher Dienste bei Cybersicherheitsvorfällen, um so zum reibungslosen Funktionieren ***der*** Wirtschaft und Gesellschaft ***der Union*** beizutragen.	(1) Ziel der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates[11]***, gemeinhin als „NIS-Richtlinie“ bekannt,*** war der unionsweite Aufbau von Cybersicherheitskapazitäten, die Eindämmung von Bedrohungen für Netz- und Informationssysteme, die zur Erbringung wesentlicher Dienste in Schlüsselsektoren verwendet werden, und die Sicherstellung der Kontinuität solcher Dienste bei Cybersicherheitsvorfällen, um so ***zur Sicherheit der Union und*** zum reibungslosen Funktionieren ***ihrer*** Wirtschaft und Gesellschaft beizutragen.
[11] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).	[11] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

Änderungsantrag 3

Vorschlag für eine Richtlinie
Erwägung 3

Vorschlag der Kommission	*Geänderter Text*
(3) Netz- und Informationssysteme sind durch den schnellen digitalen Wandel und die Vernetzung der Gesellschaft zu einem zentralen Bestandteil des Alltags und für den grenzüberschreitenden Austausch geworden. Diese Entwicklung hat zu einer Ausweitung der Bedrohungslage im Bereich der Cybersicherheit geführt und neue Herausforderungen mit sich gebracht, die in allen Mitgliedstaaten entsprechende koordinierte und innovative Reaktionen erfordern. Die Anzahl, Tragweite, Komplexität, Häufigkeit und Auswirkungen von Cybersicherheitsvorfällen nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen dar. Im Ergebnis können Cybersicherheitsvorfälle die Ausübung wirtschaftlicher Tätigkeiten im Binnenmarkt beeinträchtigen, finanzielle Verluste verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft und Gesellschaft der Union großen Schaden zufügen. Heute sind daher im Bereich Cybersicherheit Vorsorge und Wirksamkeit wichtiger denn je für das reibungslose Funktionieren des Binnenmarkts.	(3) Netz- und Informationssysteme sind durch den schnellen digitalen Wandel und die Vernetzung der Gesellschaft zu einem zentralen Bestandteil des Alltags und für den grenzüberschreitenden Austausch geworden. Diese Entwicklung hat zu einer Ausweitung der Bedrohungslage im Bereich der Cybersicherheit geführt und neue Herausforderungen mit sich gebracht, die in allen Mitgliedstaaten entsprechende koordinierte und innovative Reaktionen erfordern. Die Anzahl, Tragweite, Komplexität, Häufigkeit und Auswirkungen von Cybersicherheitsvorfällen nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen dar. Im Ergebnis können Cybersicherheitsvorfälle die Ausübung wirtschaftlicher Tätigkeiten im Binnenmarkt beeinträchtigen, finanzielle Verluste verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft und Gesellschaft der Union großen Schaden zufügen. Heute sind daher im Bereich Cybersicherheit Vorsorge und Wirksamkeit wichtiger denn je für das reibungslose Funktionieren des Binnenmarkts. ***Darüber hinaus ist die Cybersicherheit für viele kritische Sektoren eine entscheidende Voraussetzung, um den digitalen Wandel erfolgreich zu bewältigen und die wirtschaftlichen, sozialen und dauerhaften Vorteile der Digitalisierung voll zu nutzen.***

Änderungsantrag 4

Vorschlag für eine Richtlinie
Erwägung 3 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(3a) Cybersicherheitsvorfälle und -krisen großen Ausmaßes auf Unionsebene erfordern aufgrund der starken Interdependenz zwischen Sektoren und Ländern ein koordiniertes Vorgehen, um eine schnelle und wirksame Reaktion zu gewährleisten. Die Verfügbarkeit widerstandsfähiger Netze und Informationssysteme sowie die Verfügbarkeit, Vertraulichkeit und Integrität von Daten sind für die Sicherheit der Union innerhalb und außerhalb ihrer Grenzen von entscheidender Bedeutung, da Cyberbedrohungen auch von außerhalb der Union ausgehen könnten. Das Bestreben der Union, eine stärkere geopolitische Rolle einzunehmen, hängt auch von einer glaubwürdigen Cyberabwehr und -abschreckung ab, wozu auch die Fähigkeit gehört, böswillige Handlungen zeitnah und wirksam zu erkennen und angemessen darauf zu reagieren.

Änderungsantrag 5

Vorschlag für eine Richtlinie
Erwägung 5

Vorschlag der Kommission	*Geänderter Text*
(5) All diese Unterschiede führen zu einer Fragmentierung des Binnenmarkts und können sich nachteilig auf dessen Funktionieren auswirken und aufgrund der Anwendung unterschiedlicher Normen insbesondere die grenzüberschreitende Erbringung von Diensten und das Niveau der Cyberresilienz beeinträchtigen. Ziel der vorliegenden Richtlinie ist, diese großen Unterschiede zwischen den Mitgliedstaaten zu beseitigen, indem insbesondere Mindestvorschriften für einen funktionierenden und koordinierten Rechtsrahmen festgelegt werden,	(5) All diese Unterschiede führen zu einer Fragmentierung des Binnenmarkts und können sich nachteilig auf dessen Funktionieren auswirken und aufgrund der Anwendung unterschiedlicher Normen insbesondere die grenzüberschreitende Erbringung von Diensten und das Niveau der Cyberresilienz beeinträchtigen. ***Letztendlich könnten diese Unterschiede zu einer höheren Anfälligkeit einiger Mitgliedstaaten gegenüber Cybersicherheitsbedrohungen führen, deren Auswirkungen auf die gesamte Union übergreifen könnten.*** Ziel der

Mechanismen für die wirksame Zusammenarbeit zwischen den zuständigen Behörden in den einzelnen Mitgliedstaaten vorgesehen werden, die Liste der Sektoren und Tätigkeiten, die Pflichten im Hinblick auf die Cybersicherheit unterliegen, aktualisiert wird und wirksame Abhilfemaßnahmen und Sanktionen, die für die wirksame Durchsetzung dieser Verpflichtungen von entscheidender Bedeutung sind, eingeführt werden. Daher sollte die Richtlinie (EU) 2016/1148 aufgehoben und durch die vorliegende Richtlinie ersetzt werden.

vorliegenden Richtlinie ist, diese großen Unterschiede zwischen den Mitgliedstaaten zu beseitigen, indem insbesondere Mindestvorschriften für einen funktionierenden und koordinierten Rechtsrahmen festgelegt werden, Mechanismen für die wirksame Zusammenarbeit zwischen den zuständigen Behörden in den einzelnen Mitgliedstaaten vorgesehen werden, die Liste der Sektoren und Tätigkeiten, die Pflichten im Hinblick auf die Cybersicherheit unterliegen, aktualisiert wird und wirksame Abhilfemaßnahmen und Sanktionen, die für die wirksame Durchsetzung dieser Verpflichtungen von entscheidender Bedeutung sind, eingeführt werden. Daher sollte die Richtlinie (EU) 2016/1148 aufgehoben und durch die vorliegende Richtlinie ***(NIS-2-Richtlinie)*** ersetzt werden.

Änderungsantrag 6

Vorschlag für eine Richtlinie
Erwägung 6

Vorschlag der Kommission	*Geänderter Text*
(6) Im Einklang mit dem Unionsrecht bleibt die Möglichkeit der Mitgliedstaaten, die für die Wahrung ihrer wesentlichen Sicherheitsinteressen und den Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit erforderlichen Maßnahmen zu ergreifen und die Ermittlung, Feststellung und Verfolgung von Straftaten zuzulassen, von der vorliegenden Richtlinie unberührt. Nach Artikel 346 AEUV ist kein Mitgliedstaat verpflichtet, Auskünfte zu erteilen, deren Preisgabe seinen wesentlichen Sicherheitsinteressen widerspräche. In diesem Zusammenhang sind nationale und Unionsvorschriften zum Schutz von Verschlusssachen, Geheimhaltungsvereinbarungen und informelle Geheimhaltungsvereinbarungen wie das sogenannte Traffic Light	(6) Im Einklang mit dem Unionsrecht bleibt die Möglichkeit der Mitgliedstaaten, die für die Wahrung ihrer wesentlichen Sicherheitsinteressen und den Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit erforderlichen Maßnahmen zu ergreifen und die ***Verhütung,*** Ermittlung, Feststellung und Verfolgung von Straftaten zuzulassen, von der vorliegenden Richtlinie unberührt. Nach Artikel 346 AEUV ist kein Mitgliedstaat verpflichtet, Auskünfte zu erteilen, deren Preisgabe seinen wesentlichen Sicherheitsinteressen widerspräche. In diesem Zusammenhang sind nationale und Unionsvorschriften zum Schutz von Verschlusssachen, Geheimhaltungsvereinbarungen und informelle Geheimhaltungsvereinbarungen wie das sogenannte Traffic Light

Protocol[14] von Bedeutung.

[14] Mithilfe des Traffic Light Protocol (TLP) kann jemand, der Informationen weitergibt, die Empfänger über etwaige Einschränkungen bei der weiteren Verbreitung dieser Informationen informieren. Es wird in fast allen CSIRT-Gemeinschaften und einigen Informationsaustausch- und -analysezentren (Information Sharing and Analysis Centres – ISACs) genutzt.

Protocol[14] von Bedeutung.

[14] Mithilfe des Traffic Light Protocol (TLP) kann jemand, der Informationen weitergibt, die Empfänger über etwaige Einschränkungen bei der weiteren Verbreitung dieser Informationen informieren. Es wird in fast allen CSIRT-Gemeinschaften und einigen Informationsaustausch- und -analysezentren (Information Sharing and Analysis Centres – ISACs) genutzt.

Änderungsantrag 7

Vorschlag für eine Richtlinie
Erwägung 7

Vorschlag der Kommission	*Geänderter Text*
(7) Mit der Aufhebung der Richtlinie (EU) 2016/1148 sollte der Anwendungsbereich nach Sektoren aus den in den Erwägungsgründen 4 bis 6 dargelegten Gründen auf einen größeren Teil der Wirtschaft ausgeweitet werden. Die Liste der Sektoren, die unter die Richtlinie (EU) 2016/1148 fallen, sollte daher erweitert werden, um eine umfassende Abdeckung der Sektoren und Dienste zu gewährleisten, die im Binnenmarkt für grundlegende gesellschaftliche und wirtschaftliche Tätigkeiten von entscheidender Bedeutung sind. Bei den ***Vorschriften*** sollte nicht danach unterschieden werden, ob es sich bei den Einrichtungen um Betreiber wesentlicher Dienste oder um Anbieter digitaler Dienste handelt. Diese Differenzierung hat sich als überholt erwiesen, da sie nicht die tatsächliche Bedeutung der Sektoren oder Dienste für die gesellschaftlichen und wirtschaftlichen Tätigkeiten im Binnenmarkt widerspiegelt.	(7) Mit der Aufhebung der Richtlinie (EU) 2016/1148 sollte der Anwendungsbereich nach Sektoren aus den in den Erwägungsgründen 4 bis 6 dargelegten Gründen auf einen größeren Teil der Wirtschaft ausgeweitet werden. Die Liste der Sektoren, die unter die Richtlinie (EU) 2016/1148 fallen, sollte daher erweitert werden, um eine umfassende Abdeckung der Sektoren und Dienste zu gewährleisten, die im Binnenmarkt für grundlegende gesellschaftliche und wirtschaftliche Tätigkeiten von entscheidender Bedeutung sind. Bei den ***Risikomanagementanforderungen und Meldepflichten*** sollte nicht danach unterschieden werden, ob es sich bei den Einrichtungen um Betreiber wesentlicher Dienste oder um Anbieter digitaler Dienste handelt. Diese Differenzierung hat sich als überholt erwiesen, da sie nicht die tatsächliche Bedeutung der Sektoren oder Dienste für die gesellschaftlichen und wirtschaftlichen Tätigkeiten im Binnenmarkt widerspiegelt.

Änderungsantrag 8

Vorschlag für eine Richtlinie
Erwägung 8

Vorschlag der Kommission	*Geänderter Text*
(8) Gemäß der Richtlinie (EU) 2016/1148 waren die Mitgliedstaaten dafür zuständig zu bestimmen, welche Einrichtungen die Kriterien für die Einstufung als Betreiber wesentlicher Dienste erfüllen („Ermittlungsprozess“). Um die diesbezüglichen großen Unterschiede zwischen den Mitgliedstaaten zu beheben und für alle relevanten Einrichtungen Rechtssicherheit hinsichtlich der Risikomanagementanforderungen und der Meldepflichten zu gewährleisten, sollte ein einheitliches Kriterium dafür festgelegt werden, welche Einrichtungen in den Anwendungsbereich der vorliegenden Richtlinie fallen. Dieses Kriterium sollte in der Anwendung des Schwellenwerts für die Größe bestehen, nach der alle mittleren und großen Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission[15], die in den Sektoren tätig sind oder die Art von Diensten erbringen, die unter die vorliegende Richtlinie fallen, in den Anwendungsbereich der Richtlinie fallen. ***Die Mitgliedstaaten sollten nicht verpflichtet sein, eine Liste der Einrichtungen zu erstellen, die dieses allgemein anwendbare größenbezogene Kriterium erfüllen.***	(8) Gemäß der Richtlinie (EU) 2016/1148 waren die Mitgliedstaaten dafür zuständig zu bestimmen, welche Einrichtungen die Kriterien für die Einstufung als Betreiber wesentlicher Dienste erfüllen („Ermittlungsprozess“). Um die diesbezüglichen großen Unterschiede zwischen den Mitgliedstaaten zu beheben und für alle relevanten Einrichtungen Rechtssicherheit hinsichtlich der Risikomanagementanforderungen und der Meldepflichten zu gewährleisten, sollte ein einheitliches Kriterium dafür festgelegt werden, welche Einrichtungen in den Anwendungsbereich der vorliegenden Richtlinie fallen. Dieses Kriterium sollte in der Anwendung des Schwellenwerts für die Größe bestehen, nach der alle mittleren und großen Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission[15], die in den Sektoren tätig sind oder die Art von Diensten erbringen, die unter die vorliegende Richtlinie fallen, in den Anwendungsbereich der Richtlinie fallen.
[15] Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).	[15] Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).

Änderungsantrag 9

Vorschlag für eine Richtlinie
Erwägung 9

Vorschlag der Kommission	*Geänderter Text*
(9) Allerdings sollten auch Klein- und Kleinsteinrichtungen, die bestimmte Kriterien erfüllen, nach denen sie eine Schlüsselrolle für die Wirtschaft oder Gesellschaft des betreffenden Mitgliedstaats oder für bestimmte Sektoren oder Arten von Diensten spielen, von der vorliegenden Richtlinie erfasst werden. ***Die Mitgliedstaaten sollten für die Erstellung einer Liste solcher Einrichtungen zuständig sein und diese der Kommission übermitteln.***	(9) Allerdings sollten auch Klein- und Kleinsteinrichtungen, die bestimmte Kriterien erfüllen, nach denen sie eine Schlüsselrolle für die Wirtschaft oder Gesellschaft des betreffenden Mitgliedstaats oder für bestimmte Sektoren oder Arten von Diensten spielen, von der vorliegenden Richtlinie erfasst werden.

Änderungsantrag 10

Vorschlag für eine Richtlinie
Erwägung 9 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(9a) Die Mitgliedstaaten sollten eine Liste aller wesentlichen und wichtigen Einrichtungen erstellen. Diese Liste sollte die Einrichtungen, die die allgemein geltenden größenbezogenen Kriterien erfüllen, sowie Klein- und Kleinstunternehmen enthalten, die bestimmte Kriterien erfüllen, die ihrer Schlüsselrolle für die Wirtschaft oder Gesellschaft der Mitgliedstaaten entsprechen. Damit die Soforteinsatzteams für IT-Sicherheitsvorfälle (CSIRTs) und die zuständigen Behörden Unterstützung leisten und die Einrichtungen vor Cyber-Vorfällen warnen können, die sie betreffen könnten, ist es wichtig, dass diese Behörden über die richtigen Kontaktdaten der Einrichtungen verfügen. Wesentliche und wichtige Einrichtungen sollten daher den zuständigen Behörden mindestens die folgenden Informationen übermitteln: Name der Einrichtung, Anschrift und aktuelle Kontaktdaten, darunter E-Mail-Adressen, IP-Bereiche, Telefonnummern,

sowie relevante(n) Sektor(en) und Teilsektor(en) gemäß den Anhängen I und II. Die Einrichtungen sollten die zuständigen Behörden über jede Änderung dieser Informationen unterrichten. Die Mitgliedstaaten sollten unverzüglich sicherstellen, dass diese Informationen über eine zentrale Anlaufstelle problemlos bereitgestellt werden können. Zu diesem Zweck sollte die ENISA in Zusammenarbeit mit der Kooperationsgruppe unverzüglich Leitlinien und Vorlagen für die Meldepflichten herausgeben. Die Mitgliedstaaten sollten der Kommission und der Kooperationsgruppe die Anzahl der wesentlichen und wichtigen Einrichtungen mitteilen. Die Mitgliedstaaten sollten der Kommission für die Zwecke der in dieser Richtlinie genannten Überprüfung auch die Namen der kleinen Unternehmen und Kleinstunternehmen mitteilen, die als wesentliche und wichtige Einrichtungen identifiziert wurden, damit die Kommission die Kohärenz zwischen den Ansätzen der Mitgliedstaaten bewerten kann. Diese Informationen sollten streng vertraulich behandelt werden.

Änderungsantrag 11

Vorschlag für eine Richtlinie
Erwägung 10

Vorschlag der Kommission	*Geänderter Text*
(10) Die Kommission ***kann*** in Zusammenarbeit mit der Kooperationsgruppe Leitlinien für die Anwendung der für ***Klein-*** und ***Kleinstunternehmen*** geltenden Kriterien herausgeben.	(10) Die Kommission ***sollte*** in Zusammenarbeit mit der Kooperationsgruppe ***und einschlägigen Interessenträgern*** Leitlinien für die Anwendung der für ***Kleinstunternehmen*** und ***kleine Unternehmen*** geltenden Kriterien herausgeben. ***Die Kommission sollte auch dafür sorgen, dass alle Kleinst- und Kleinunternehmen, die in den Anwendungsbereich dieser Richtlinie fallen, eine angemessene Anleitung erhalten. Die Kommission sollte mit***

Unterstützung der Mitgliedstaaten den Kleinst- und Kleinunternehmen diesbezügliche Informationen zur Verfügung stellen.

Änderungsantrag 12

Vorschlag für eine Richtlinie
Erwägung 10 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(10a) Die Kommission sollte ferner Leitlinien herausgeben, um die Mitgliedstaaten bei der korrekten Umsetzung der Bestimmungen über den Anwendungsbereich zu unterstützen und die Verhältnismäßigkeit der in dieser Richtlinie dargelegten Pflichten zu evaluieren, insbesondere in Bezug auf Einrichtungen mit komplexen Geschäftsmodellen oder Betriebsumgebungen, wobei eine Einrichtung gleichzeitig die Kriterien für wesentliche und für wichtige Einrichtungen erfüllen kann oder gleichzeitig Tätigkeiten, die in den Anwendungsbereich dieser Richtlinie fallen, und andere Tätigkeiten ausführen kann.

Änderungsantrag 13

Vorschlag für eine Richtlinie
Erwägung 12

Vorschlag der Kommission	*Geänderter Text*
(12) Durch sektorspezifische Rechtsvorschriften und Instrumente kann dazu beigetragen werden, ein hohes Maß an Cybersicherheit zu gewährleisten und gleichzeitig den Besonderheiten und Komplexitäten der Sektoren in vollem Umfang Rechnung zu tragen. Müssen wesentliche oder wichtige Einrichtungen gemäß einem sektorspezifischen Rechtsakt der Union Maßnahmen zum	(12) Durch sektorspezifische Rechtsvorschriften und Instrumente kann dazu beigetragen werden, ein hohes Maß an Cybersicherheit zu gewährleisten und gleichzeitig den Besonderheiten und Komplexitäten der Sektoren in vollem Umfang Rechnung zu tragen. ***Sektorspezifische Rechtsakte der Union, die von wesentlichen oder wichtigen Einrichtungen verlangen, Maßnahmen***

Cybersicherheitsrisikomanagement ergreifen oder Sicherheitsvorfälle ***oder erhebliche Cyberbedrohungen*** melden und ***ist dies*** in der Wirkung den in der vorliegenden Richtlinie festgelegten Verpflichtungen mindestens gleichwertig, so sollten diese sektorspezifischen Bestimmungen, einschließlich in Bezug auf Aufsicht und Durchsetzung, Anwendung finden. Die Kommission ***kann*** Leitlinien im Zusammenhang mit der Umsetzung der lex specialis herausgeben. Die vorliegende Richtlinie schließt nicht aus, dass zusätzliche sektorspezifische Rechtsakte der Union zu Maßnahmen zum Cybersicherheitsrisikomanagement und zur Meldung von Sicherheitsvorfällen erlassen werden. Die vorliegende Richtlinie berührt nicht die bestehenden Durchführungsbefugnisse, die der Kommission in einer Reihe von Sektoren, darunter Verkehr und Energie, übertragen wurden.

des Cybersicherheitsrisikomanagements zu ergreifen oder erhebliche Sicherheitsvorfälle zu melden, sollten sich, soweit möglich, der Terminologie dieser Richtlinie bedienen und auf ihre Begriffsbestimmungen verweisen. Müssen wesentliche oder wichtige Einrichtungen gemäß einem sektorspezifischen Rechtsakt der Union Maßnahmen zum Cybersicherheitsrisikomanagement ergreifen oder Sicherheitsvorfälle melden***,*** und ***sind diese Anforderungen*** in der Wirkung den in der vorliegenden Richtlinie festgelegten Verpflichtungen mindestens gleichwertig ***und gelten sie für die Gesamtheit der Sicherheitsaspekte der von wesentlichen und wichtigen Einrichtungen erbrachten Tätigkeiten und Dienste***, so sollten diese sektorspezifischen Bestimmungen, einschließlich in Bezug auf Aufsicht und Durchsetzung, Anwendung finden. Die Kommission ***sollte umfassende*** Leitlinien im Zusammenhang mit der Umsetzung der lex specialis herausgeben ***und dabei die einschlägigen Stellungnahmen, das Fachwissen und die bewährten Verfahren der ENISA und der Kooperationsgruppe berücksichtigen***. Die vorliegende Richtlinie schließt nicht aus, dass zusätzliche sektorspezifische Rechtsakte der Union zu Maßnahmen zum Cybersicherheitsrisikomanagement und zur Meldung von Sicherheitsvorfällen***, die der Notwendigkeit eines umfassenden und kohärenten Cybersicherheitsrahmens gebührend Rechnung tragen,*** erlassen werden. Die vorliegende Richtlinie berührt nicht die bestehenden Durchführungsbefugnisse, die der Kommission in einer Reihe von Sektoren, darunter Verkehr und Energie, übertragen wurden.

Änderungsantrag 14

Vorschlag für eine Richtlinie
Erwägung 14

Vorschlag der Kommission	*Geänderter Text*
(14) Angesichts der Zusammenhänge zwischen der Cybersicherheit und der physischen Sicherheit von Einrichtungen sollte dafür gesorgt werden, dass der Ansatz der Richtlinie (EU) XXX/XXX des Europäischen Parlaments und des Rates[17] und der Ansatz der vorliegenden Richtlinie kohärent sind. Um dies zu erreichen, sollten die Mitgliedstaaten sicherstellen, dass kritische Einrichtungen und diesen gleichgestellte Einrichtungen im Sinne der Richtlinie (EU) XXX/XXX als wesentliche Einrichtungen im Sinne der vorliegenden Richtlinie gelten. Die Mitgliedstaaten sollten auch sicherstellen, dass ihre Cybersicherheitsstrategien einen politischen Rahmen für eine verstärkte Koordinierung zwischen ***der*** gemäß der vorliegenden Richtlinie zuständigen ***Behörde*** und der gemäß Richtlinie (EU) XXX/XXX zuständigen Behörde beim Informationsaustausch über Sicherheitsvorfälle und Cyberbedrohungen und bei der Wahrnehmung von Aufsichtsaufgaben vorsehen. Die gemäß diesen beiden Richtlinien zuständigen Behörden sollten zusammenarbeiten und Informationen austauschen, insbesondere in Bezug auf die Ermittlung kritischer Einrichtungen, Cyberbedrohungen, Cybersicherheitsrisiken und Sicherheitsvorfälle, die kritische Einrichtungen beeinträchtigen, sowie über die von kritischen Einrichtungen ergriffenen Cybersicherheitsmaßnahmen. Auf Ersuchen der gemäß der Richtlinie (EU) XXX/XXX zuständigen Behörden sollte den gemäß der vorliegenden Richtlinie zuständigen Behörden gestattet werden, ihre Aufsichts- und Durchsetzungsbefugnisse gegenüber einer als kritisch eingestuften wesentlichen Einrichtung auszuüben. Beide Behörden sollten zu diesem Zweck zusammenarbeiten und Informationen	(14) Angesichts der Zusammenhänge zwischen der Cybersicherheit und der physischen Sicherheit von Einrichtungen sollte dafür gesorgt werden, dass der Ansatz der Richtlinie (EU) XXX/XXX des Europäischen Parlaments und des Rates[17] und der Ansatz der vorliegenden Richtlinie kohärent sind. Um dies zu erreichen, sollten die Mitgliedstaaten sicherstellen, dass kritische Einrichtungen und diesen gleichgestellte Einrichtungen im Sinne der Richtlinie (EU) XXX/XXX als wesentliche Einrichtungen im Sinne der vorliegenden Richtlinie gelten. Die Mitgliedstaaten sollten auch sicherstellen, dass ihre Cybersicherheitsstrategien einen politischen Rahmen für eine verstärkte Koordinierung zwischen ***den*** gemäß der vorliegenden Richtlinie zuständigen ***Behörden in und zwischen den Mitgliedstaaten*** und der gemäß ***der*** Richtlinie (EU) XXX/XXX zuständigen Behörde beim Informationsaustausch über Sicherheitsvorfälle und Cyberbedrohungen und bei der Wahrnehmung von Aufsichtsaufgaben vorsehen. Die gemäß diesen beiden Richtlinien zuständigen Behörden sollten ***unverzüglich*** zusammenarbeiten und Informationen austauschen, insbesondere in Bezug auf die Ermittlung kritischer Einrichtungen, Cyberbedrohungen, Cybersicherheitsrisiken und Sicherheitsvorfälle, die kritische Einrichtungen beeinträchtigen, sowie über die von kritischen Einrichtungen ergriffenen Cybersicherheitsmaßnahmen. Auf Ersuchen der gemäß der Richtlinie (EU) XXX/XXX zuständigen Behörden sollte den gemäß der vorliegenden Richtlinie zuständigen Behörden gestattet werden, ihre Aufsichts- und Durchsetzungsbefugnisse gegenüber einer als kritisch eingestuften wesentlichen Einrichtung auszuüben. Beide Behörden sollten zu diesem Zweck

austauschen.

[17] [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].

zusammenarbeiten und ***möglichst in Echtzeit*** Informationen austauschen.

[17] [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].

Änderungsantrag 15

Vorschlag für eine Richtlinie
Erwägung 15

Vorschlag der Kommission	*Geänderter Text*
(15) Die Beibehaltung eines zuverlässigen, resilienten und sicheren Domänennamensystems (DNS) ist ein Schlüsselfaktor für die Wahrung der Integrität des Internets und von entscheidender Bedeutung für dessen kontinuierlichen und stabilen Betrieb, von dem die digitale Wirtschaft und Gesellschaft abhängig ist. Daher sollte die vorliegende Richtlinie für ***alle Anbieter von DNS-Diensten entlang der DNS-Auflösungskette gelten, einschließlich Betreibern von Root-Namenservern, Namenservern*** der Domäne oberster Stufe (TLD-Namenservern)***, autoritativen Namenservern für*** Domänennamen ***und rekursiven Resolvern***.	(15) Die Beibehaltung eines zuverlässigen, resilienten und sicheren Domänennamensystems (DNS) ist ein Schlüsselfaktor für die Wahrung der Integrität des Internets und von entscheidender Bedeutung für dessen kontinuierlichen und stabilen Betrieb, von dem die digitale Wirtschaft und Gesellschaft abhängig ist. Daher sollte die vorliegende Richtlinie für ***Namenserver*** der Domäne oberster Stufe (TLD-Namenservern)***, öffentlich zugängliche rekursive Dienste zur Auflösung*** von ***Domänennamen für Internet-Endnutzer und autoritative Dienste zur Auflösung von*** Domänennamen ***gelten. Diese Richtlinie gilt nicht für Root-Namenserver***.

Änderungsantrag 16

Vorschlag für eine Richtlinie
Erwägung 19

Vorschlag der Kommission	*Geänderter Text*
(19) Anbieter von Postdiensten im Sinne der Richtlinie 97/67/EG des Europäischen Parlaments und des Rates[18] sowie Anbieter von Express- und Kurierdiensten sollten der vorliegenden Richtlinie unterliegen, wenn sie mindestens einen der Schritte in	(19) Anbieter von Postdiensten im Sinne der Richtlinie 97/67/EG des Europäischen Parlaments und des Rates[18] sowie Anbieter von Express- und Kurierdiensten sollten der vorliegenden Richtlinie unterliegen, wenn sie mindestens einen der Schritte in

der Postzustellkette und insbesondere Abholung, Sortierung oder Zustellung, einschließlich Abholung durch den Empfänger, anbieten. Transportdienste, die nicht in Verbindung mit einem dieser Schritte erbracht werden, sollten nicht unter Postdienste fallen.	der Postzustellkette und insbesondere Abholung, Sortierung oder Zustellung, einschließlich Abholung durch den Empfänger, anbieten***, wobei das Ausmaß ihrer Abhängigkeit von Netzwerk- und Informationssystemen berücksichtigt werden sollte***. Transportdienste, die nicht in Verbindung mit einem dieser Schritte erbracht werden, sollten nicht unter Postdienste fallen.
[18] Richtlinie 97/67/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über gemeinsame Vorschriften für die Entwicklung des Binnenmarktes der Postdienste der Gemeinschaft und die Verbesserung der Dienstequalität (ABl. L 15 vom 21.1.1998, S. 14).	[18] Richtlinie 97/67/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über gemeinsame Vorschriften für die Entwicklung des Binnenmarktes der Postdienste der Gemeinschaft und die Verbesserung der Dienstequalität (ABl. L 15 vom 21.1.1998, S. 14).

Änderungsantrag 17

Vorschlag für eine Richtlinie
Erwägung 20

Vorschlag der Kommission	*Geänderter Text*
(20) Diese wachsenden gegenseitigen Abhängigkeiten sind das Ergebnis eines sich über immer mehr Grenzen hinweg erstreckenden und zunehmend interdependenten Dienstleistungsnetzes, das zentrale Infrastrukturen in der gesamten Union nutzt, und zwar in den Sektoren Energie, Verkehr, digitale Infrastruktur, Trinkwasser und Abwasser, Gesundheit, bestimmten Bereichen der öffentlichen Verwaltung sowie im Weltraumsektor, soweit es um die Erbringung bestimmter Dienste geht, die von Bodeninfrastrukturen abhängig sind, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden; damit sind Infrastrukturen ausgenommen, die sich im Eigentum der Union befinden oder von der Union oder in ihrem Namen im Rahmen ihrer Weltraumprogramme	(20) Diese wachsenden gegenseitigen Abhängigkeiten sind das Ergebnis eines sich über immer mehr Grenzen hinweg erstreckenden und zunehmend interdependenten Dienstleistungsnetzes, das zentrale Infrastrukturen in der gesamten Union nutzt, und zwar in den Sektoren Energie, Verkehr, digitale Infrastruktur, Trinkwasser und Abwasser, Gesundheit, bestimmten Bereichen der öffentlichen Verwaltung sowie im Weltraumsektor, soweit es um die Erbringung bestimmter Dienste geht, die von Bodeninfrastrukturen abhängig sind, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden; damit sind Infrastrukturen ausgenommen, die sich im Eigentum der Union befinden oder von der Union oder in ihrem Namen im Rahmen ihrer Weltraumprogramme

verwaltet oder betrieben werden. Wegen dieser gegenseitigen Abhängigkeiten kann jede Störung, auch wenn sie anfänglich auf eine Einrichtung oder einen Sektor beschränkt ist, zu breiteren Kaskadeneffekten führen, die weitreichende und lang anhaltende negative Auswirkungen auf die Erbringung von Dienstleistungen im gesamten Binnenmarkt haben können. Die COVID-19-Pandemie ***hat*** gezeigt, wie anfällig unsere zunehmend interdependenten Gesellschaften für Risiken mit geringer Eintrittswahrscheinlichkeit sind.

verwaltet oder betrieben werden. Wegen dieser gegenseitigen Abhängigkeiten kann jede Störung, auch wenn sie anfänglich auf eine Einrichtung oder einen Sektor beschränkt ist, zu breiteren Kaskadeneffekten führen, die weitreichende und lang anhaltende negative Auswirkungen auf die Erbringung von Dienstleistungen im gesamten Binnenmarkt haben können. Die ***verstärkten Angriffe auf Netz- und Informationssysteme während der*** COVID-19-Pandemie ***haben*** gezeigt, wie anfällig unsere zunehmend interdependenten Gesellschaften für Risiken mit geringer Eintrittswahrscheinlichkeit sind.

Änderungsantrag 18

Vorschlag für eine Richtlinie
Erwägung 24

Vorschlag der Kommission	*Geänderter Text*
(24) Die Mitgliedstaaten sollten über angemessene technische und organisatorische Kapazitäten zur Prävention, Erkennung, Reaktion und Abschwächung von Sicherheitsvorfällen und Risiken bei Netz- und Informationssystemen verfügen. Die Mitgliedstaaten sollten daher ***sicherstellen, dass sie über gut funktionierende Reaktionsteams für IT-Sicherheitsvorfälle – Computer Security Incident Response Teams (CSIRTs) oder auch Computer Emergency Response Teams (CERTs) genannt – verfügen, die*** die grundlegenden Anforderungen erfüllen, damit wirksame und kompatible Kapazitäten zur Bewältigung von Sicherheitsvorfällen und Risiken und eine effiziente Zusammenarbeit auf Unionsebene gewährleistet sind. Um das Vertrauensverhältnis zwischen den Einrichtungen und den CSIRTs zu stärken, sollten die Mitgliedstaaten in Fällen, in denen ein CSIRT Teil der zuständigen	(24) Die Mitgliedstaaten sollten über angemessene technische und organisatorische Kapazitäten zur Prävention, Erkennung, Reaktion und Abschwächung von Sicherheitsvorfällen und Risiken bei Netz- und Informationssystemen verfügen. Die Mitgliedstaaten sollten daher ***ein oder mehrere CSIRTs im Sinne dieser Richtlinie benennen und sicherstellen, dass diese gut funktionieren und*** die grundlegenden Anforderungen erfüllen, damit wirksame und kompatible Kapazitäten zur Bewältigung von Sicherheitsvorfällen und Risiken und eine effiziente Zusammenarbeit auf Unionsebene gewährleistet sind***. Die Mitgliedstaaten können auch bestehende Computer-Notfallteams (CERTs) als CSIRTs benennen.*** Um das Vertrauensverhältnis zwischen den Einrichtungen und den CSIRTs zu stärken, sollten die Mitgliedstaaten in Fällen, in denen ein CSIRT Teil der zuständigen

Behörde ist, eine funktionale Trennung zwischen den operativen Aufgaben der CSIRTs, insbesondere in Bezug auf den Informationsaustausch und die Unterstützung der Einrichtungen, und den Aufsichtstätigkeiten der zuständigen Behörden in Erwägung ziehen.	Behörde ist, eine funktionale Trennung zwischen den operativen Aufgaben der CSIRTs, insbesondere in Bezug auf den Informationsaustausch und die Unterstützung der Einrichtungen, und den Aufsichtstätigkeiten der zuständigen Behörden in Erwägung ziehen.

Änderungsantrag 19

Vorschlag für eine Richtlinie
Erwägung 25

Vorschlag der Kommission	*Geänderter Text*
(25) In Bezug auf personenbezogene Daten sollten CSIRTs in der Lage sein, im Einklang mit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[19] im Namen und auf Ersuchen einer unter die vorliegende Richtlinie fallenden Einrichtung eine proaktive Überprüfung der für die Bereitstellung ihrer Dienste verwendeten Netz- und Informationssysteme auf Schwachstellen vorzunehmen. Die Mitgliedstaaten sollten für alle sektorbezogenen CSIRTs ein vergleichbares Niveau an technischen Kapazitäten anstreben. Die Mitgliedstaaten können die Agentur der Europäischen Union für Cybersicherheit (ENISA) um Unterstützung bei der Einsetzung nationaler CSIRTs ersuchen.	(25) In Bezug auf personenbezogene Daten sollten CSIRTs in der Lage sein, im Einklang mit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[19] im Namen und auf Ersuchen einer unter die vorliegende Richtlinie fallenden Einrichtung ***oder im Falle einer ernsthaften Bedrohung der nationalen Sicherheit*** eine proaktive Überprüfung der für die Bereitstellung ihrer Dienste verwendeten Netz- und Informationssysteme auf Schwachstellen vorzunehmen. Die Mitgliedstaaten sollten für alle sektorbezogenen CSIRTs ein vergleichbares Niveau an technischen Kapazitäten anstreben. Die Mitgliedstaaten können die Agentur der Europäischen Union für Cybersicherheit (ENISA) um Unterstützung bei der Einsetzung nationaler CSIRTs ersuchen.
[19] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).	19 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

Änderungsantrag 20

Vorschlag für eine Richtlinie
Erwägung 25 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(25a) CSIRTs sollten in der Lage sein, auf Ersuchen einer Einrichtung alle mit dem Internet verbundenen Anlagen innerhalb und außerhalb der Geschäftsräume kontinuierlich zu kontaktieren, zu inventarisieren, zu verwalten und zu überwachen, um das organisatorische Gesamtrisiko für neu entdeckte Sicherheitslücken in der Lieferkette oder kritische Schwachstellen zu verstehen. Die Information darüber, ob eine Einrichtung über eine privilegierte Verwaltungsschnittstelle verfügt, wirkt sich auf die Geschwindigkeit der Durchführung von Abhilfemaßnahmen aus.

Änderungsantrag 21

Vorschlag für eine Richtlinie
Erwägung 26

Vorschlag der Kommission	*Geänderter Text*
(26) Wegen der Bedeutung der internationalen Zusammenarbeit im Bereich Cybersicherheit sollten die CSIRTs sich zusätzlich zum durch die vorliegende Richtlinie geschaffenen CSIRT-Netzwerk an internationalen Kooperationsnetzen beteiligen können.	(26) Wegen der Bedeutung der internationalen Zusammenarbeit im Bereich Cybersicherheit sollten die CSIRTs sich zusätzlich zum durch die vorliegende Richtlinie geschaffenen CSIRT-Netzwerk an internationalen Kooperationsnetzen ***– auch mit CSIRTs aus Drittländern, wenn der Informationsaustausch auf Gegenseitigkeit beruht und für die Sicherheit der Bürger und Einrichtungen von Nutzen ist –*** beteiligen können***, um zur Erarbeitung von Normen der Union beizutragen, die die Cybersicherheitslandschaft auf internationaler Ebene prägen können. Die Mitgliedstaaten könnten auch die Möglichkeiten einer verstärkten Zusammenarbeit mit gleichgesinnten***

Partnerländern und internationalen Organisationen prüfen, um multilaterale Vereinbarungen über Normen für den Cyberbereich, verantwortungsbewusstes staatliches und nichtstaatliches Verhalten im Cyberraum und eine wirksame globale E-Governance sicherzustellen sowie einen offenen, freien, stabilen und sicheren Cyberraum auf der Grundlage des Völkerrechts zu schaffen.

Änderungsantrag 22

Vorschlag für eine Richtlinie
Erwägung 26 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(26a) Cyber-Hygienemaßnahmen bilden die Grundlage für den Schutz von Netzwerk- und Informationssysteminfrastrukturen, Hardware, Software und Online-Anwendungssicherheit sowie von Geschäfts- oder Endnutzerdaten, derer sich Einrichtungen bedienen. Cyber-Hygienemaßnahmen, die eine Reihe von grundlegenden Verfahren umfassen, wie z. B. Software- und Hardware-Updates, Passwortänderungen, die Verwaltung neuer Installationen, die Einschränkung von Zugriffskonten auf Administratorenebene und die Sicherung von Daten, ermöglichen einen proaktiven Rahmen für die Bereitschaft und die allgemeine Sicherheit im Falle von Sicherheitsvorfällen oder Bedrohungen. Die ENISA sollte die Cyber-Hygienemaßnahmen der Mitgliedstaaten überwachen und bewerten und unionsweite Systeme erkunden, um grenzüberschreitende Prüfungen zu ermöglichen, die die Gleichwertigkeit unabhängig von den Anforderungen der Mitgliedstaaten sicherstellen.

Änderungsantrag 23

Vorschlag für eine Richtlinie
Erwägung 26 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	(26b) Der Einsatz von künstlicher Intelligenz (KI) in der Cybersicherheit hat das Potenzial, die Aufdeckung zu verbessern und Angriffe auf Netz- und Informationssysteme zu stoppen, so dass Ressourcen für komplexere Angriffe eingesetzt werden können. Die Mitgliedstaaten sollten daher in ihren nationalen Strategien den Einsatz (halb)automatisierter Werkzeuge für die Cybersicherheit und den Austausch von Daten fördern, die für die Schulung und Verbesserung automatisierter Werkzeuge für die Cybersicherheit erforderlich sind. Um die sich unter Umständen aus KI-gestützten Systemen ergebenden Risiken eines unzulässigen Eingriffs in die Rechte und Freiheiten natürlicher Personen zu mindern, gelten die Anforderungen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen gemäß Artikel 25 der Verordnung (EU) 2016/679. Die Integration geeigneter Schutzmaßnahmen wie Pseudonymisierung, Verschlüsselung, Datengenauigkeit und Datenminimierung könnten solche Risiken weiter mindern.

Änderungsantrag 24

Vorschlag für eine Richtlinie
Erwägung 26 c (neu)

Vorschlag der Kommission	*Geänderter Text*
	(26c) Open-Source-Cybersicherheitswerkzeuge und -Anwendungen können zu einem höheren Maß an Transparenz beitragen und sich positiv auf die Effizienz industrieller Innovationen auswirken. Offene Standards erleichtern die Interoperabilität zwischen Sicherheitstools, was der

Sicherheit der Interessenträger aus der Industrie zugutekommt. Open-Source-Cybersicherheitswerkzeuge und -anwendungen können die breitere Entwicklergemeinschaft nutzen und die Einrichtungen in die Lage versetzen, eine Diversifizierung der Anbieter anzustreben und offene Sicherheitsstrategien zu verfolgen. Offene Sicherheit kann zu einem transparenteren Überprüfungsprozess von Werkzeugen für die Cybersicherheit und zu einem von der Gemeinschaft gesteuerten Prozess der Aufdeckung von Schwachstellen führen. Die Mitgliedstaaten sollten daher den Einsatz von Open-Source-Software und offenen Standards fördern, indem sie Maßnahmen zur Nutzung offener Daten und Open-Source als Teil der Sicherheit durch Transparenz verfolgen. Maßnahmen zur Förderung der Annahme und nachhaltigen Nutzung von Open-Source-Cybersicherheitswerkzeugen sind besonders für kleine und mittlere Unternehmen (KMU) wichtig, bei denen erhebliche Implementierungskosten anfallen, die durch die Reduzierung des Bedarfs an spezifischen Anwendungen oder Werkzeugen minimiert werden könnten.

Änderungsantrag 25

Vorschlag für eine Richtlinie
Erwägung 26 d (neu)

Vorschlag der Kommission	*Geänderter Text*
	(26d) Öffentlich-private Partnerschaften (ÖPP) im Bereich der Cybersicherheit können den richtigen Rahmen für den Wissensaustausch, die Weitergabe von bewährten Verfahren und die Schaffung einer gemeinsamen Verständnisebene zwischen allen Beteiligten bieten. Die Mitgliedstaaten sollten im Rahmen ihrer nationalen Cybersicherheitsstrategien Maßnahmen ergreifen, die die

	Einrichtung von cybersicherheitsspezifischen ÖPP unterstützen. Diese Maßnahmen sollten unter anderem den Anwendungsbereich und die beteiligten Akteure, das Verwaltungsmodell, die verfügbaren Finanzierungsoptionen und das Zusammenspiel der beteiligten Akteure präzisieren. ÖPP können das Fachwissen privatwirtschaftlicher Einrichtungen nutzen, um die zuständigen Behörden der Mitgliedstaaten bei der Entwicklung modernster Dienste und Prozesse zu unterstützen, unter anderem in den Bereichen Informationsaustausch, Frühwarnungen, Übungen zu Cyberbedrohungen und -vorfällen, Krisenmanagement und Resilienzplanung.

Änderungsantrag 26

Vorschlag für eine Richtlinie
Erwägung 27

Vorschlag der Kommission	*Geänderter Text*
(27) Im Einklang mit dem Anhang der Empfehlung (EU) 2017/1548 der Kommission für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen („Konzeptentwurf“)[20] sollte der Begriff „Sicherheitsvorfall großen Ausmaßes“ einen Sicherheitsvorfall bezeichnen, der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat oder der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt. Je nach Ursache und Auswirkung können sich Sicherheitsvorfälle großen Ausmaßes verschärfen und zu echten Krisen entwickeln, die das reibungslose Funktionieren des Binnenmarkts verhindern. Angesichts der großen Tragweite und des, in den meisten Fällen, grenzübergreifenden Charakters solcher Sicherheitsvorfälle sollten die	(27) Im Einklang mit dem Anhang der Empfehlung (EU) 2017/1548 der Kommission für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen („Konzeptentwurf“)[20] sollte der Begriff „Sicherheitsvorfall großen Ausmaßes“ einen Sicherheitsvorfall bezeichnen, der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat oder der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt. Je nach Ursache und Auswirkung können sich Sicherheitsvorfälle großen Ausmaßes verschärfen und zu echten Krisen entwickeln, die das reibungslose Funktionieren des Binnenmarkts verhindern ***oder ernsthafte, die öffentliche Sicherheit betreffende Risiken für Einrichtungen und Bürger in mehreren Mitgliedstaaten oder in der gesamten***

Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union auf technischer, operativer und politischer Ebene zusammenarbeiten, um die Reaktion unionsweit angemessen zu koordinieren.

[20] Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (ABl. L 239 vom 19.9.2017, S. 36).

Union darstellen. Angesichts der großen Tragweite und des, in den meisten Fällen, grenzübergreifenden Charakters solcher Sicherheitsvorfälle sollten die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union auf technischer, operativer und politischer Ebene zusammenarbeiten, um die Reaktion unionsweit angemessen zu koordinieren.

[20] Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (ABl. L 239 vom 19.9.2017, S. 36).

Änderungsantrag 27

Vorschlag für eine Richtlinie
Erwägung 27 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(27a) Die Mitgliedstaaten sollten in ihren nationalen Cybersicherheitsstrategien auf die besonderen Cybersicherheitsbedürfnisse von KMU eingehen. KMU stellen im Kontext der Union einen großen Prozentsatz des Industrie-/Geschäftsmarktes, und sie haben damit zu kämpfen, sich an ein neues Geschäftsgebaren in einer stärker vernetzten Welt anzupassen und sich in der digitalen Umgebung zurechtzufinden, in der Mitarbeiter von zu Hause aus arbeiten und Geschäfte zunehmend online getätigt werden. Einige KMU stehen vor besonderen Herausforderungen im Bereich der Cybersicherheit, wie z. B. geringes Cyber-Bewusstsein, fehlende IT-Sicherheit aus der Ferne, hohe Kosten für Cybersicherheitslösungen und ein erhöhtes Maß an Bedrohungen, wie z. B. Ransomware, für die sie Anleitung und Unterstützung erhalten sollten. Die

	Mitgliedstaaten sollten eine zentrale Anlaufstelle für Cybersicherheit für KMU einrichten, die entweder Beratung und Unterstützung für KMU anbietet oder sie an die geeigneten Stellen für Beratung und Unterstützung in Fragen der Cybersicherheit weiterleitet. Die Mitgliedstaaten werden ermutigt, auch kleinen Unternehmen und Kleinstunternehmen, die nicht über diese Fähigkeiten verfügen, Dienste wie die Konfiguration von Websites und die Aktivierung der Protokollierung anzubieten.

Änderungsantrag 28

Vorschlag für eine Richtlinie
Erwägung 27 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	(27b) Die Mitgliedstaaten sollten Maßnahmen zur Förderung einer aktiven Cyberverteidigung als Teil ihrer nationalen Cybersicherheitsstrategien ergreifen. Aktive Cyberverteidigung ist die proaktive Verhütung, Erkennung, Überwachung, Analyse und Abschwächung von Sicherheitsverletzungen im Netzwerk, kombiniert mit der Nutzung von Kapazitäten, die innerhalb und außerhalb des Opfernetzwerks eingesetzt werden. Die Fähigkeit, Bedrohungsinformationen und -analysen, Warnungen zu Cyber-Aktivitäten und Reaktionsmaßnahmen schnell und automatisch auszutauschen und zu verstehen, ist entscheidend, um eine einheitliche Vorgehensweise bei der erfolgreichen Erkennung, Verhütung und Bekämpfung von Angriffen gegen Netz- und Informationssysteme zu ermöglichen. Die aktive Cyberabwehr basiert auf einer defensiven Strategie, die offensive Maßnahmen gegen kritische zivile Infrastrukturen ausschließt.

Änderungsantrag 29

Vorschlag für eine Richtlinie
Erwägung 28

Vorschlag der Kommission	*Geänderter Text*
(28) Da durch die Ausnutzung von Schwachstellen in Netz- und Informationssystemen erhebliche Störungen und Schäden verursacht werden können, ist die rasche Erkennung und Behebung dieser Schwachstellen ein wichtiger Faktor bei der Verringerung des Cybersicherheitsrisikos. Einrichtungen, die solche Systeme entwickeln, sollten daher geeignete Verfahren für die Behandlung von entdeckten Schwachstellen festlegen. Da Schwachstellen häufig von Dritten (meldenden Einrichtungen) entdeckt und gemeldet (offengelegt) werden, sollte der Hersteller oder Anbieter von IKT-Produkten oder -Diensten auch Verfahren einführen, damit er von Dritten Informationen über Schwachstellen entgegennehmen kann. Diesbezüglich enthalten die internationalen Normen ISO/IEC 30111 und ISO/IEC 29417 Leitlinien für die Behandlung von Schwachstellen bzw. die Offenlegung von Schwachstellen. ***In Bezug auf die Offenlegung von Schwachstellen ist die*** Koordinierung zwischen meldenden Einrichtungen und Herstellern oder Anbietern von IKT-Produkten oder -Diensten besonders wichtig. Die koordinierte Offenlegung von Schwachstellen erfolgt in einem strukturierten Prozess, in dem den Organisationen Schwachstellen in einer Weise gemeldet werden, die der Organisation die Diagnose und Behebung der Schwachstelle ermöglicht, bevor detaillierte Informationen über die Schwachstelle an Dritte oder die Öffentlichkeit weitergegeben werden. Die koordinierte Offenlegung von Schwachstellen sollte auch die Koordinierung zwischen der meldenden	(28) Da durch die Ausnutzung von Schwachstellen in Netz- und Informationssystemen erhebliche Störungen und Schäden verursacht werden können, ist die rasche Erkennung und Behebung dieser Schwachstellen ein wichtiger Faktor bei der Verringerung des Cybersicherheitsrisikos. Einrichtungen, die solche Systeme entwickeln, sollten daher geeignete Verfahren für die Behandlung von entdeckten Schwachstellen festlegen. Da Schwachstellen häufig von Dritten (meldenden Einrichtungen) entdeckt und gemeldet (offengelegt) werden, sollte der Hersteller oder Anbieter von IKT-Produkten oder -Diensten auch Verfahren einführen, damit er von Dritten Informationen über Schwachstellen entgegennehmen kann. Diesbezüglich enthalten die internationalen Normen ISO/IEC 30111 und ISO/IEC 29417 Leitlinien für die Behandlung von Schwachstellen bzw. die Offenlegung von Schwachstellen. ***Eine stärkere*** Koordinierung zwischen meldenden Einrichtungen und Herstellern oder Anbietern von IKT-Produkten oder -Diensten ***ist*** besonders wichtig***, um den freiwilligen Rahmen für die Offenlegung von Schwachstellen attraktiver zu machen***. Die koordinierte Offenlegung von Schwachstellen erfolgt in einem strukturierten Prozess, in dem den Organisationen Schwachstellen in einer Weise gemeldet werden, die der Organisation die Diagnose und Behebung der Schwachstelle ermöglicht, bevor detaillierte Informationen über die Schwachstelle an Dritte oder die Öffentlichkeit weitergegeben werden. Die koordinierte Offenlegung von Schwachstellen sollte auch die

Einrichtung und der Organisation in Bezug auf den Zeitplan für die Behebung und Veröffentlichung von Schwachstellen umfassen.

Koordinierung zwischen der meldenden Einrichtung und der Organisation in Bezug auf den Zeitplan für die Behebung und Veröffentlichung von Schwachstellen umfassen.

Änderungsantrag 30

Vorschlag für eine Richtlinie
Erwägung 28 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(28a) Die Kommission, die ENISA und die Mitgliedstaaten sollten die internationale Anpassung an Normen und vorliegende bewährte Verfahren der Branche im Bereich des Risikomanagements weiterhin fördern, beispielsweise in den Bereichen Bewertungen der Sicherheit der Lieferkette, Informationsaustausch und Offenlegung von Schwachstellen.

Änderungsantrag 31

Vorschlag für eine Richtlinie
Erwägung 29

Vorschlag der Kommission	*Geänderter Text*
(29) Die Mitgliedstaaten sollten daher Maßnahmen ergreifen, um eine koordinierte Offenlegung von Schwachstellen zu erleichtern, indem sie eine einschlägige nationale Strategie festlegen. ***In diesem Zusammenhang*** sollten die Mitgliedstaaten ***ein CSIRT benennen***, ***das*** die ***Rolle des „Koordinators“ übernimmt und gegebenenfalls zwischen den meldenden Einrichtungen und den Herstellern oder Anbietern von IKT-Produkten oder -Diensten vermittelt***. ***Zu den Aufgaben des als Koordinator benannten CSIRT sollte insbesondere gehören, betroffene*** Einrichtungen ***zu ermitteln*** und ***zu kontaktieren, meldende Einrichtungen zu***	(29) Die Mitgliedstaaten sollten daher ***in Zusammenarbeit mit der ENISA*** Maßnahmen ergreifen, um eine koordinierte Offenlegung von Schwachstellen zu erleichtern, indem sie eine einschlägige nationale Strategie festlegen. ***Im Rahmen dieser nationalen Strategie*** sollten die Mitgliedstaaten ***auf Probleme eingehen***, ***auf*** die ***Forschende, die im Bereich Schwachstellen tätig sind, stoßen***. Einrichtungen und ***natürliche Personen***, die Schwachstellen ***erforschen***, ***können in einigen Mitgliedstaaten unter Umständen strafrechtlich und zivilrechtlich zur Verantwortung gezogen werden. Den Mitgliedstaaten wird daher nahegelegt***, ***Leitlinien für den Verzicht***

unterstützen, ***Zeitpläne für*** die ***Offenlegung auszuhandeln und das Vorgehen bei*** Schwachstellen ***zu koordinieren***, ***die mehrere Organisationen betreffen (Offenlegung von Schwachstellen, die mehrere Parteien betreffen). Betreffen Schwachstellen mehrere Hersteller oder Anbieter von IKT-Produkten oder -Diensten***, ***die in mehr als einem Mitgliedstaat niedergelassen sind, sollten*** die ***benannten CSIRTs aus den betroffenen Mitgliedstaaten*** im ***Rahmen des CSIRT-Netzwerkes zusammenarbeiten***.

auf Strafverfolgung und die ***Nichthaftung in Bezug auf Forschung*** im ***Bereich der Informationssicherheit herauszugeben***.

Änderungsantrag 32

Vorschlag für eine Richtlinie
Erwägung 29 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(29a) Die Mitgliedstaaten sollten ein CSIRT benennen, das die Rolle des „Koordinators“ übernimmt und gegebenenfalls zwischen den meldenden Einrichtungen und den Herstellern oder Anbietern von IKT-Produkten oder -Diensten, die wahrscheinlich von der Schwachstelle betroffen sind, vermittelt. Zu den Aufgaben des als Koordinator benannten CSIRT sollte insbesondere gehören, betroffene Einrichtungen zu ermitteln und zu kontaktieren, meldende Einrichtungen zu unterstützen, Zeitpläne für die Offenlegung auszuhandeln und das Vorgehen bei Schwachstellen zu koordinieren, die mehrere Organisationen betreffen (Offenlegung von Schwachstellen, die mehrere Parteien betreffen). Betreffen Schwachstellen mehrere Hersteller oder Anbieter von IKT-Produkten oder -Diensten, die in mehr als einem Mitgliedstaat niedergelassen sind, sollten die benannten CSIRTs aus den betroffenen Mitgliedstaaten im Rahmen des CSIRT-Netzwerkes zusammenarbeiten.

Änderungsantrag 33

Vorschlag für eine Richtlinie
Erwägung 30

Vorschlag der Kommission	*Geänderter Text*
(30) Der rechtzeitige Zugang zu korrekten Informationen über Schwachstellen, die IKT-Produkte und -Dienste beeinträchtigen, trägt zu einem besseren Cybersicherheitsrisikomanagement bei. ***In dieser Hinsicht sind*** öffentlich zugängliche Informationen über Schwachstellen nicht nur für Einrichtungen und deren Nutzer, sondern auch für die zuständigen nationalen Behörden und die CSIRTs ein wichtiges Instrument. Aus diesem Grund sollte die ENISA ***ein Schwachstellenregister*** einrichten, in dem wesentliche und wichtige Einrichtungen und deren Anbieter sowie, auf freiwilliger Basis, Einrichtungen, die nicht in den Anwendungsbereich der vorliegenden Richtlinie fallen, Schwachstellen offenlegen und Informationen über die Schwachstellen bereitstellen, die es den Nutzern ermöglichen, geeignete Abhilfemaßnahmen zu ergreifen.	(30) Der rechtzeitige Zugang zu korrekten Informationen über Schwachstellen, die IKT-Produkte und -Dienste beeinträchtigen, trägt zu einem besseren Cybersicherheitsrisikomanagement bei. Öffentlich zugängliche Informationen über Schwachstellen ***sind*** nicht nur für Einrichtungen und deren Nutzer, sondern auch für die zuständigen nationalen Behörden und die CSIRTs ein wichtiges Instrument. Aus diesem Grund sollte die ENISA ***eine Datenbank für Schwachstellen*** einrichten, in dem wesentliche und wichtige Einrichtungen und deren Anbieter sowie, auf freiwilliger Basis, Einrichtungen, die nicht in den Anwendungsbereich der vorliegenden Richtlinie fallen, Schwachstellen offenlegen und Informationen über die Schwachstellen bereitstellen, die es den Nutzern ermöglichen, geeignete Abhilfemaßnahmen zu ergreifen. ***Das Ziel dieser Datenbank ist es, die einzigartigen Herausforderungen zu bewältigen, die sich aus den Cybersicherheitsrisiken für europäische Einrichtungen ergeben. Darüber hinaus sollte die ENISA ein Verfahren für den Veröffentlichungsprozess einführen, um den Einrichtungen Zeit zu geben, Maßnahmen zur Behebung ihrer Schwachstellen zu ergreifen und moderne Cybersicherheitsmaßnahmen sowie maschinenlesbare Datensätze und entsprechende Schnittstellen (APIs) einzusetzen. Zur Förderung einer Kultur der Offenlegung von Schwachstellen sollte eine Offenlegung ohne nachteilige Folgen für die meldende Einrichtung erfolgen.***

Änderungsantrag 34

Vorschlag für eine Richtlinie
Erwägung 31

Vorschlag der Kommission	*Geänderter Text*
(31) ***Es gibt zwar bereits ähnliche Register oder Datenbanken für Schwachstellen, aber diese werden von Einrichtungen betrieben und gepflegt, die nicht in der Union niedergelassen sind. Ein*** von der ENISA ***gepflegtes europäisches Schwachstellenregister würde*** für ***mehr Transparenz in Bezug auf den Prozess der Veröffentlichung vor der offiziellen Offenlegung der Schwachstelle sorgen*** und ***die Resilienz im Falle*** von ***Störungen oder Unterbrechungen bei der Erbringung ähnlicher Dienste verbessern***. ***Um Doppelarbeit zu vermeiden und im Interesse der größtmöglichen Komplementarität,*** sollte die ENISA die Möglichkeit prüfen, Vereinbarungen über eine strukturierte Zusammenarbeit mit ähnlichen Registern in Drittländern zu schließen.	(31) ***Die*** von der ENISA ***gepflegte europäische Datenbank*** für Schwachstellen ***sollte das Register „Common Vulnerabilities and Exposures“ (Bekannte Schwachstellen und Anfälligkeiten) nutzen, indem sie dessen Rahmen*** für ***die Identifizierung, Verfolgung*** und ***Bewertung*** von ***Schwachstellen verwendet***. ***Darüber hinaus*** sollte die ENISA die Möglichkeit prüfen, Vereinbarungen über eine strukturierte Zusammenarbeit mit ***anderen*** ähnlichen Registern ***oder Datenbanken*** in Drittländern zu schließen***, um Doppelarbeit zu vermeiden und Komplementarität anzustreben***.

Änderungsantrag 35

Vorschlag für eine Richtlinie
Erwägung 33

Vorschlag der Kommission	*Geänderter Text*
(33) Bei der Ausarbeitung von Leitfäden sollte die Kooperationsgruppe konsequent nationale Lösungen und Erfahrungen erfassen, die Auswirkungen ihrer Vorgaben auf nationale Ansätze bewerten, Herausforderungen bei der Umsetzung erörtern und spezifische Empfehlungen für eine bessere Umsetzung bestehender Vorschriften formulieren.	(33) Bei der Ausarbeitung von Leitfäden sollte die Kooperationsgruppe konsequent nationale Lösungen und Erfahrungen erfassen, die Auswirkungen ihrer Vorgaben auf nationale Ansätze bewerten, Herausforderungen bei der Umsetzung erörtern und spezifische Empfehlungen für eine bessere Umsetzung bestehender Vorschriften formulieren***, insbesondere hinsichtlich der Erleichterung der Angleichung bei der Umsetzung dieser Richtlinie zwischen den Mitgliedstaaten. Die Kooperationsgruppe sollte auch eine Bestandsaufnahme der nationalen***

	Lösungen vornehmen, um die Kompatibilität von Cybersicherheitslösungen zu fördern, die für jeden einzelnen Sektor in der gesamten Union angewandt werden. Dies gilt insbesondere für Sektoren mit internationalem und grenzüberschreitendem Charakter .

Änderungsantrag 36

Vorschlag für eine Richtlinie
Erwägung 34

Vorschlag der Kommission	*Geänderter Text*
(34) Die Kooperationsgruppe sollte ein flexibles Forum bleiben und in der Lage sein, unter Berücksichtigung der verfügbaren Ressourcen auf sich ändernde und neue politische Prioritäten und Herausforderungen zu reagieren. Sie sollte regelmäßige gemeinsame Sitzungen mit einschlägigen privaten Interessenträgern aus der gesamten Union organisieren, um die Tätigkeiten der Gruppe zu erörtern und Beiträge zu neuen politischen Herausforderungen einzuholen. Um die Zusammenarbeit auf Unionsebene zu verbessern, sollte die Gruppe in Erwägung ziehen, mit Cybersicherheitspolitik befasste Einrichtungen und Agenturen der Union, etwa ***das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3)***, die Agentur der Europäischen Union für Flugsicherheit (EASA) und die Agentur der Europäischen Union für das Weltraumprogramm (EUSPA), zur Teilnahme an ihrer Arbeit einzuladen.	(34) Die Kooperationsgruppe sollte ein flexibles Forum bleiben und in der Lage sein, unter Berücksichtigung der verfügbaren Ressourcen auf sich ändernde und neue politische Prioritäten und Herausforderungen zu reagieren. Sie sollte regelmäßige gemeinsame Sitzungen mit einschlägigen privaten Interessenträgern aus der gesamten Union organisieren, um die Tätigkeiten der Gruppe zu erörtern und Beiträge zu neuen politischen Herausforderungen einzuholen. Um die Zusammenarbeit auf Unionsebene zu verbessern, sollte die Gruppe in Erwägung ziehen, ***einschlägige,*** mit Cybersicherheitspolitik befasste Einrichtungen und Agenturen der Union, ***wie*** etwa ***Europol***, die Agentur der Europäischen Union für Flugsicherheit (EASA) und die Agentur der Europäischen Union für das Weltraumprogramm (EUSPA), zur Teilnahme an ihrer Arbeit einzuladen.

Änderungsantrag 37

Vorschlag für eine Richtlinie
Erwägung 35

Vorschlag der Kommission	*Geänderter Text*
(35) Die zuständigen Behörden und	(35) Die zuständigen Behörden und

CSIRTs sollten befugt sein, an Austauschprogrammen für Bedienstete aus anderen Mitgliedstaaten teilzunehmen, um die Zusammenarbeit zu verbessern. Die zuständigen Behörden sollten Maßnahmen ergreifen, damit die Bediensteten aus anderen Mitgliedstaaten bei den Tätigkeiten der aufnehmenden zuständigen Behörde konstruktiv mitwirken können.	CSIRTs sollten befugt sein, an Austauschprogrammen für Bedienstete aus anderen Mitgliedstaaten teilzunehmen, ***im Rahmen strukturierter Regeln und Mechanismen, die den Anwendungsbereich und gegebenenfalls die erforderliche Sicherheitsüberprüfung der an solchen Austauschprogrammen teilnehmenden Beamten untermauern,*** um die Zusammenarbeit zu verbessern ***und das Vertrauen unter den Mitgliedstaaten zu stärken***. Die zuständigen Behörden sollten Maßnahmen ergreifen, damit die Bediensteten aus anderen Mitgliedstaaten bei den Tätigkeiten der aufnehmenden zuständigen Behörde ***oder des CSIRT*** konstruktiv mitwirken können.

Änderungsantrag 38

Vorschlag für eine Richtlinie
Erwägung 36

Vorschlag der Kommission	*Geänderter Text*
(36) Die Union sollte gegebenenfalls internationale Übereinkünfte mit Drittländern oder internationalen Organisationen im Einklang mit Artikel 218 AEUV schließen, in denen deren Beteiligung an bestimmten Tätigkeiten der Kooperationsgruppe und dem CSIRT-Netzwerk ermöglicht und geregelt wird. Solche Übereinkünfte sollten einen angemessenen Datenschutz gewährleisten.	(36) Die Union sollte gegebenenfalls internationale Übereinkünfte mit Drittländern oder internationalen Organisationen im Einklang mit Artikel 218 AEUV schließen, in denen deren Beteiligung an bestimmten Tätigkeiten der Kooperationsgruppe und dem CSIRT-Netzwerk ermöglicht und geregelt wird. Solche Übereinkünfte sollten ***die Interessen der Union wahren und*** einen angemessenen Datenschutz gewährleisten. ***Dies schließt nicht das Recht der Mitgliedstaaten aus, mit gleichgesinnten Drittländern bei der Verwaltung von Schwachstellen und von Cybersicherheitsrisiken zusammenzuarbeiten und die Berichterstattung und den allgemeinen Informationsaustausch im Einklang mit dem Recht der Union zu erleichtern.***

Änderungsantrag 39

Vorschlag für eine Richtlinie
Erwägung 38

Vorschlag der Kommission	*Geänderter Text*
(38) Für die Zwecke der vorliegenden Richtlinie sollte sich der Begriff „Risiko“ auf das Potenzial für Verluste oder Störungen infolge eines Cybersicherheitsvorfalls beziehen und als Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des besagten Sicherheitsvorfalls ausgedrückt werden.	***entfällt***

Änderungsantrag 40

Vorschlag für eine Richtlinie
Erwägung 39

Vorschlag der Kommission	*Geänderter Text*
(39) Für die Zwecke der vorliegenden Richtlinie sollte sich der Begriff „Beinahe-Vorfälle“ auf ein Ereignis beziehen, das das Potenzial gehabt hätte, Schäden zu verursachen, dessen vollständiger Eintritt jedoch verhindert wurde.	***entfällt***

Änderungsantrag 41

Vorschlag für eine Richtlinie
Erwägung 40

Vorschlag der Kommission	*Geänderter Text*
(40) Das Risikomanagement sollte auch Maßnahmen zur Ermittlung jeder Gefahr ***eines Sicherheitsvorfalls***, ***zur*** Verhinderung**,** Aufdeckung und ***Bewältigung von*** Sicherheitsvorfällen sowie ***der*** Minderung ihrer Folgen umfassen. Die Sicherheit von Netz- und Informationssystemen sollte sich auch auf gespeicherte, übermittelte und verarbeitete Daten erstrecken.	(40) Das Risikomanagement sollte auch Maßnahmen zur Ermittlung jeder Gefahr ***von Sicherheitsvorfällen***, ***zu ihrer*** Verhinderung ***und*** Aufdeckung**,** ***zur Reaktion auf sie*** und ***zur Wiederherstellung nach*** Sicherheitsvorfällen sowie ***zur*** Minderung ihrer Folgen umfassen. Die Sicherheit von Netz- und Informationssystemen sollte sich auch auf gespeicherte, übermittelte und

verarbeitete Daten erstrecken. ***Diese Systeme sollten eine systemische Analyse vorsehen, bei der die verschiedenen Prozesse und die Wechselwirkungen zwischen den Teilsystemen aufgeschlüsselt werden und der menschliche Faktor berücksichtigt wird, um ein vollständiges Bild der Sicherheit des Informationssystems zu erhalten.***

Änderungsantrag 42

Vorschlag für eine Richtlinie
Erwägung 41

Vorschlag der Kommission	*Geänderter Text*
(41) Damit keine unverhältnismäßige finanzielle und administrative Belastung für wesentliche und wichtige Einrichtungen entsteht, sollten die Anforderungen an das Cybersicherheitsrisikomanagement in einem angemessenen Verhältnis zu den Risiken stehen, denen das betreffende Netz- und Informationssystem ausgesetzt ist; dabei wird dem bei solchen Maßnahmen geltenden neuesten Stand Rechnung getragen.	(41) Damit keine unverhältnismäßige finanzielle und administrative Belastung für wesentliche und wichtige Einrichtungen entsteht, sollten die Anforderungen an das Cybersicherheitsrisikomanagement in einem angemessenen Verhältnis zu den Risiken stehen, denen das betreffende Netz- und Informationssystem ausgesetzt ist; dabei wird dem bei solchen Maßnahmen geltenden neuesten Stand ***sowie europäischen oder internationalen Standards, wie etwa ISO31000 und ISA/IEC 27005*** Rechnung getragen.

Änderungsantrag 43

Vorschlag für eine Richtlinie
Erwägung 43

Vorschlag der Kommission	*Geänderter Text*
(43) Besonders wichtig ist die Bewältigung von Cybersicherheitsrisiken, die die Lieferkette von Einrichtungen und deren Beziehungen zu den Lieferanten betreffen, da sich die Vorfälle häufen, bei denen Einrichtungen Opfer von ***Cyberangriffen*** werden und es böswilligen Akteuren gelingt, die Sicherheit der Netz- und Informationssysteme zu	(43) Besonders wichtig ist die Bewältigung von Cybersicherheitsrisiken, die die Lieferkette von Einrichtungen und deren Beziehungen zu den Lieferanten***, z. B. Anbietern von Datenspeicherungs- und -verarbeitungsdiensten oder von verwalteten Sicherheitsdiensten,*** betreffen, da sich die Vorfälle häufen, bei denen Einrichtungen Opfer von ***Angriffen auf***

beeinträchtigen, indem Schwachstellen im Zusammenhang mit den Produkten und Dienstleistungen Dritter ausgenutzt werden. Die Einrichtungen sollten daher die Gesamtqualität der Produkte und Cybersicherheitsverfahren ihrer Lieferanten und Diensteanbieter, einschließlich ihrer sicheren Entwicklungsprozesse, bewerten und berücksichtigen.

Netz- und Informationssysteme werden und es böswilligen Akteuren gelingt, die Sicherheit der Netz- und Informationssysteme zu beeinträchtigen, indem Schwachstellen im Zusammenhang mit den Produkten und Dienstleistungen Dritter ausgenutzt werden. Die Einrichtungen sollten daher die Gesamtqualität ***und Widerstandsfähigkeit*** der Produkte und ***Dienstleistungen, die darin enthaltenen Cybersicherheitsmaßnahmen und die*** Cybersicherheitsverfahren ihrer Lieferanten und Diensteanbieter, einschließlich ihrer sicheren Entwicklungsprozesse, bewerten und berücksichtigen. ***Die Einrichtungen sollten insbesondere dazu angehalten werden, Maßnahmen zur Cybersicherheit in die vertraglichen Vereinbarungen mit ihren Lieferanten und Diensteanbietern der ersten Ebene einzubeziehen. Die Einrichtungen könnten auch die Cybersicherheitsrisiken berücksichtigen, die von Lieferanten und Dienstleistern anderer Ebenen ausgehen.***

Änderungsantrag 44

Vorschlag für eine Richtlinie
Erwägung 44

Vorschlag der Kommission	*Geänderter Text*
(44) Unter den Diensteanbietern spielen die Anbieter verwalteter Sicherheitsdienste (Managed Security Services Providers, MSSP) in Bereichen wie Reaktion auf Sicherheitsvorfälle, Penetrationstests, Sicherheitsaudits und Beratung eine überaus wichtige Rolle, indem sie Einrichtungen bei deren Bemühungen um die Erkennung und Bewältigung von Sicherheitsvorfällen unterstützen. Allerdings sind auch die MSSP selbst das Ziel von Cyberangriffen und stellen durch ihre enge Einbindung in die Tätigkeiten der Betreiber ein besonderes Cybersicherheitsrisiko dar. Die	(44) Unter den Diensteanbietern spielen die Anbieter verwalteter Sicherheitsdienste (Managed Security Services Providers, MSSP) in Bereichen wie Reaktion auf Sicherheitsvorfälle, Penetrationstests, Sicherheitsaudits und Beratung eine überaus wichtige Rolle, indem sie Einrichtungen bei deren Bemühungen um die ***Verhütung,*** Erkennung und Bewältigung von ***Sicherheitsvorfällen sowie die Wiederherstellung nach*** Sicherheitsvorfällen unterstützen. Allerdings sind auch die MSSP selbst das Ziel von Cyberangriffen und stellen durch ihre enge Einbindung in die Tätigkeiten der

Einrichtungen sollten daher bei der Wahl eines MSSP erhöhte Sorgfalt walten lassen.

Betreiber ein besonderes Cybersicherheitsrisiko dar. Die Einrichtungen sollten daher bei der Wahl eines MSSP erhöhte Sorgfalt walten lassen.

Änderungsantrag 45

Vorschlag für eine Richtlinie
Erwägung 45

Vorschlag der Kommission	*Geänderter Text*
(45) Die Einrichtungen sollten sich auch mit Cybersicherheitsrisiken befassen, die sich aus ihren Interaktionen und Beziehungen zu anderen interessierten Kreisen in einem weiter gefassten Ökosystem ergeben. Insbesondere sollten die Einrichtungen durch geeignete Maßnahmen sicherstellen, dass ihre Zusammenarbeit mit Hochschul- und Forschungseinrichtungen ihrer Cybersicherheitsstrategie entspricht und dabei bewährte Verfahren befolgt werden, was den sicheren Zugang zu sowie die Verbreitung von Informationen im Allgemeinen und den Schutz des geistigen Eigentums im Besonderen angeht. Auch sollten in Anbetracht der Bedeutung und des Wertes von Daten für die Tätigkeiten der Einrichtungen letztere alle geeigneten Cybersicherheitsmaßnahmen ergreifen, wenn sie die Datenverarbeitungs- und -analysedienste Dritter in Anspruch nehmen.	(45) Die Einrichtungen sollten sich auch mit Cybersicherheitsrisiken befassen, die sich aus ihren Interaktionen und Beziehungen zu anderen interessierten Kreisen in einem weiter gefassten Ökosystem ergeben***, unter anderem zur Abwehr von Wirtschaftsspionage und zum Schutz von Geschäftsgeheimnissen***. Insbesondere sollten die Einrichtungen durch geeignete Maßnahmen sicherstellen, dass ihre Zusammenarbeit mit Hochschul- und Forschungseinrichtungen ihrer Cybersicherheitsstrategie entspricht und dabei bewährte Verfahren befolgt werden, was den sicheren Zugang zu sowie die Verbreitung von Informationen im Allgemeinen und den Schutz des geistigen Eigentums im Besonderen angeht. Auch sollten in Anbetracht der Bedeutung und des Wertes von Daten für die Tätigkeiten der Einrichtungen letztere alle geeigneten Cybersicherheitsmaßnahmen ergreifen, wenn sie die Datenverarbeitungs- und -analysedienste Dritter in Anspruch nehmen.

Änderungsantrag 46

Vorschlag für eine Richtlinie
Erwägung 45 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(45a) Die Einrichtungen sollten sich einer großen Bandbreite grundlegender Praktiken im Bereich der Cyberhygiene

bedienen, wie Null-Vertrauen-Architektur, Software-Updates, Gerätekonfiguration, Netzwerksegmentierung, Identitäts- und Zugangsmanagement oder Nutzerbewusstsein sowie Schulungen zu Cyberbedrohungen im Zusammenhang mit E-Mails in Unternehmen, Phishing oder Social Engineering. Außerdem sollten die Einrichtungen ihre eigenen Cybersicherheitskapazitäten bewerten und gegebenenfalls die Integration von Technologien zur Verbesserung der Cybersicherheit anstreben, die von künstlicher Intelligenz oder maschinellen Lernsystemen gestützt werden, um ihre Kapazitäten und den Schutz von Netzwerkarchitekturen zu automatisieren.

Änderungsantrag 47

Vorschlag für eine Richtlinie
Erwägung 46

Vorschlag der Kommission	*Geänderter Text*
(46) Um die Hauptrisiken für die Lieferkette weiter anzugehen und den Einrichtungen in den unter diese Richtlinie fallenden Sektoren dabei zu helfen, Cybersicherheitsrisiken in Bezug auf die Lieferkette und die Lieferanten angemessen zu beherrschen, sollte die Kooperationsgruppe, an der die einschlägigen nationalen Behörden beteiligt sind, in Zusammenarbeit mit der Kommission und der ENISA koordinierte ***sektorenbezogene*** Lieferketten-Risikobewertungen – wie im Fall der 5G-Netze gemäß der einschlägigen Empfehlung (EU) 2019/534[21] – durchführen, um für jeden Sektor die kritischen IKT-Dienste, -Systeme oder -Produkte sowie relevante Bedrohungen und Schwachstellen zu ermitteln.	(46) Um die Hauptrisiken für die Lieferkette weiter anzugehen und den Einrichtungen in den unter diese Richtlinie fallenden Sektoren dabei zu helfen, Cybersicherheitsrisiken in Bezug auf die Lieferkette und die Lieferanten angemessen zu beherrschen, sollte die Kooperationsgruppe, an der die einschlägigen nationalen Behörden beteiligt sind, in Zusammenarbeit mit der Kommission und der ENISA koordinierte Lieferketten-Risikobewertungen – wie im Fall der 5G-Netze gemäß der einschlägigen Empfehlung (EU) 2019/534[21] – durchführen, um für jeden Sektor die kritischen IKT- ***und IKS-***Dienste, -Systeme oder -Produkte sowie relevante Bedrohungen und Schwachstellen zu ermitteln. ***Bei solchen Risikobewertungen sollten Maßnahmen, Pläne zur Risikominderung und bewährte Verfahren gegen kritische Abhängigkeiten, potenzielle einzelne***

Fehlerquellen, Bedrohungen, Schwachstellen und andere Risiken im Zusammenhang mit der Lieferkette ermittelt werden, und es sollte nach Möglichkeiten gesucht werden, ihre breitere Anwendung durch die Einrichtungen zu fördern. Zu den potenziellen nichttechnischen Risikofaktoren wie ungebührlicher Einflussnahme eines Drittlandes auf Lieferanten und Diensteanbieter, insbesondere im Fall von alternativen Governance-Modellen, zählen versteckte Schwachstellen oder Hintertüren sowie potenzielle systemische Versorgungsunterbrechungen, insbesondere im Fall von Zwangsbindungen an bestimmte Technologien oder Anbieter.

[21] (EU) 2019/534 der Kommission vom 26. März 2019 Cybersicherheit der 5G-Netze (ABl. L 88 vom 29.3.2019, S. 42).

[21] (EU) 2019/534 der Kommission vom 26. März 2019 Cybersicherheit der 5G-Netze (ABl. L 88 vom 29.3.2019, S. 42).

Änderungsantrag 48

Vorschlag für eine Richtlinie
Erwägung 47

Vorschlag der Kommission	*Geänderter Text*
(47) Bei den Lieferketten-Risikobewertungen unter Berücksichtigung der Besonderheiten des jeweiligen Sektors sollte sowohl technischen wie auch gegebenenfalls nichttechnischen Faktoren Rechnung getragen werden, einschließlich derer, die in der Empfehlung (EU) 2019/534, in der EU-weit koordinierten Risikobewertung zur Cybersicherheit in 5G-Netzen sowie in dem von der Kooperationsgruppe vereinbarten EU-Instrumentarium für die 5G-Cybersicherheit definiert sind. Bei der Ermittlung der Lieferketten, die einer koordinierten Risikobewertung unterzogen werden sollten, sollten folgende Kriterien berücksichtigt werden: (i) der Umfang, in	(47) Bei den Lieferketten-Risikobewertungen unter Berücksichtigung der Besonderheiten des jeweiligen Sektors sollte sowohl technischen wie auch gegebenenfalls nichttechnischen Faktoren Rechnung getragen werden, einschließlich derer, die in der Empfehlung (EU) 2019/534, in der EU-weit koordinierten Risikobewertung zur Cybersicherheit in 5G-Netzen sowie in dem von der Kooperationsgruppe vereinbarten EU-Instrumentarium für die 5G-Cybersicherheit definiert sind. Bei der Ermittlung der Lieferketten, die einer koordinierten Risikobewertung unterzogen werden sollten, sollten folgende Kriterien berücksichtigt werden: i) der Umfang, in

dem wesentliche und wichtige Einrichtungen bestimmte kritische IKT-Dienste, -Systeme oder -Produkte nutzen und auf sie angewiesen sind; (ii) die Bedeutung bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte für die Ausführung kritischer oder sensibler Funktionen, einschließlich der Verarbeitung personenbezogener Daten; iii) die Verfügbarkeit alternativer IKT-Dienste, -Systeme oder -Produkte; iv) die Resilienz der gesamten Lieferkette von IKT-Diensten, -Systemen oder -Produkten gegen destabilisierende Ereignisse und v) die potenzielle künftige Bedeutung neuer IKT-Dienste, -Systeme oder -Produkte für die Tätigkeiten der Einrichtungen.	dem wesentliche und wichtige Einrichtungen bestimmte kritische IKT-Dienste, -Systeme oder -Produkte nutzen und auf sie angewiesen sind; ii) die Bedeutung bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte für die Ausführung kritischer oder sensibler Funktionen, einschließlich der Verarbeitung personenbezogener Daten; iii) die Verfügbarkeit alternativer IKT-Dienste, -Systeme oder -Produkte; iv) die Resilienz der gesamten Lieferkette von IKT-Diensten, -Systemen oder -Produkten ***während ihres gesamten Lebenszyklus*** gegen destabilisierende Ereignisse und v) die potenzielle künftige Bedeutung neuer IKT-Dienste, -Systeme oder -Produkte für die Tätigkeiten der Einrichtungen. ***Besonderes Augenmerk sollte auf IKT-Dienstleistungen, -Systeme oder -Produkte gelegt werden, die speziellen Anforderungen unterliegen, die von Drittländern stammen.***

Änderungsantrag 49

Vorschlag für eine Richtlinie
Erwägung 47 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(47a) Die gemäß Artikel 22 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[1a] eingesetzte Gruppe der Interessenträger für die Cybersicherheitszertifizierung sollte eine Stellungnahme zu Sicherheitsrisikobewertungen bestimmter kritischer IKT- und IKS-Dienste, -Systeme oder -Produktlieferketten abgeben. Die Kooperationsgruppe und die ENISA sollten dieser Stellungnahme Rechnung tragen.
	[1a] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für

Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15).

Änderungsantrag 50

Vorschlag für eine Richtlinie
Erwägung 50

Vorschlag der Kommission	*Geänderter Text*
(50) Angesichts der wachsenden Bedeutung nummernunabhängiger interpersoneller Kommunikationsdienste muss sichergestellt werden, dass auch für diese Dienste angemessene Sicherheitsanforderungen entsprechend ihrer spezifischen Art und wirtschaftlichen Bedeutung gelten. Die Anbieter solcher Dienste sollten daher auch ein Sicherheitsniveau von Netz- und Informationssystemen gewährleisten, das dem bestehenden Risiko angemessen ist. Da die Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste üblicherweise keine tatsächliche Kontrolle über die Signalübertragung über Netze ausüben, kann das Risiko für solche Dienste in gewisser Hinsicht als geringer erachtet werden als für herkömmliche elektronische Kommunikationsdienste. Dasselbe gilt auch für interpersonelle Kommunikationsdienste, die Nummern nutzen und die keine tatsächliche Kontrolle über die Signalübertragung ausüben.	(50) Angesichts der wachsenden Bedeutung nummernunabhängiger interpersoneller Kommunikationsdienste muss sichergestellt werden, dass auch für diese Dienste angemessene Sicherheitsanforderungen entsprechend ihrer spezifischen Art und wirtschaftlichen Bedeutung gelten. Die Anbieter solcher Dienste sollten daher auch ein Sicherheitsniveau von Netz- und Informationssystemen gewährleisten, das dem bestehenden Risiko angemessen ist. Da die Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste üblicherweise keine tatsächliche Kontrolle über die Signalübertragung über Netze ausüben, kann das Risiko ***der Netzsicherheit*** für solche Dienste in gewisser Hinsicht als geringer erachtet werden als für herkömmliche elektronische Kommunikationsdienste. Dasselbe gilt auch für interpersonelle Kommunikationsdienste, die Nummern nutzen und die keine tatsächliche Kontrolle über die Signalübertragung ausüben. ***Da sich die Angriffsfläche jedoch immer weiter vergrößert, werden nummernunabhängige interpersonelle Kommunikationsdienste, darunter auch Messenger der sozialen Medien, zu beliebten Angriffsvektoren. Böswillige Akteure nutzen Plattformen, um zu kommunizieren und Opfer zum Öffnen***

	kompromittierter Webseiten zu verleiten, wodurch sich die Wahrscheinlichkeit von Vorfällen erhöht, bei denen persönliche Daten verwertet und damit die Sicherheit von Informationssystemen ausgenutzt wird.

Änderungsantrag 51

Vorschlag für eine Richtlinie
Erwägung 51

Vorschlag der Kommission	*Geänderter Text*
(51) Das Funktionieren des Internets ist für den Binnenmarkt wichtiger denn je. Die Dienstleistungen praktisch aller wesentlichen und wichtigen Einrichtungen hängen ihrerseits von Diensten ab, die über das Internet erbracht werden. Für die reibungslose Bereitstellung von Diensten wesentlicher und wichtiger Einrichtungen ist es wichtig, dass für ***öffentliche elektronische*** Kommunikationsnetze, z. B. Internet-Backbone- oder Seekabel, geeignete Cybersicherheitsmaßnahmen bestehen und diesbezügliche Sicherheitsvorfälle gemeldet werden.	(51) Das Funktionieren des Internets ist für den Binnenmarkt wichtiger denn je. Die Dienstleistungen praktisch aller wesentlichen und wichtigen Einrichtungen hängen ihrerseits von Diensten ab, die über das Internet erbracht werden. Für die reibungslose Bereitstellung von Diensten wesentlicher und wichtiger Einrichtungen ist es wichtig, dass für ***alle öffentlichen elektronischen*** Kommunikationsnetze, z. B. Internet-Backbone- oder Seekabel, geeignete Cybersicherheitsmaßnahmen bestehen und diesbezügliche ***erhebliche*** Sicherheitsvorfälle gemeldet werden. ***Die Mitgliedstaaten sollten sicherstellen, dass die Integrität und Verfügbarkeit dieser öffentlichen elektronischen Kommunikationsnetze aufrechterhalten wird, und sie sollten ihren Schutz vor Sabotage und Spionage als eine Frage von vitalem Sicherheitsinteresse betrachten. Informationen über Vorfälle, z. B. bei unterseeischen Kommunikationskabeln, sollten zwischen den Mitgliedstaaten aktiv ausgetauscht werden.***

Änderungsantrag 52

Vorschlag für eine Richtlinie
Erwägung 52

Vorschlag der Kommission	*Geänderter Text*
(52) Gegebenenfalls sollten die Einrichtungen die Empfänger ihrer Dienste über besondere und erhebliche Bedrohungen sowie über Maßnahmen informieren, die sie ergreifen können, um das sich daraus ergebende Risiko für sich selbst zu mindern. ***Die Verpflichtung zur Information der Empfänger über solche Bedrohungen sollte*** die Einrichtungen nicht von der Pflicht ***befreien***, auf eigene Kosten angemessene Sofortmaßnahmen zu ergreifen, um jedwede Cyberbedrohung zu verhüten oder zu beseitigen und das normale Sicherheitsniveau des Dienstes wiederherzustellen. Die Bereitstellung solcher Informationen über Sicherheitsbedrohungen ***sollte*** für die Empfänger kostenlos sein.	(52) Gegebenenfalls sollten die Einrichtungen die Empfänger ihrer Dienste über besondere und erhebliche Bedrohungen sowie über Maßnahmen informieren, die sie ergreifen können, um das sich daraus ergebende Risiko für sich selbst zu mindern. ***Dadurch sollten*** die Einrichtungen nicht von der Pflicht ***befreit werden***, auf eigene Kosten angemessene Sofortmaßnahmen zu ergreifen, um jedwede Cyberbedrohung zu verhüten oder zu beseitigen und das normale Sicherheitsniveau des Dienstes wiederherzustellen. Die Bereitstellung solcher Informationen über Sicherheitsbedrohungen für die Empfänger ***sollte*** kostenlos sein***, und die Informationen sollten in leicht verständlicher Sprache abgefasst werden***.

Änderungsantrag 53

Vorschlag für eine Richtlinie
Erwägung 53

Vorschlag der Kommission	*Geänderter Text*
(53) ***Insbesondere sollten*** die Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste die Empfänger der Dienste über besondere und erhebliche Cyberbedrohungen sowie über Maßnahmen zum Schutz von Kommunikationsinhalten, die sie treffen können, informieren, z. B. den Einsatz spezieller ***Software*** oder ***von Verschlüsselungsverfahren***.	(53) Die Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste ***sollten Sicherheit durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen implementieren und*** die Empfänger der Dienste über besondere und erhebliche Cyberbedrohungen sowie über Maßnahmen zum Schutz von Kommunikationsinhalten, die sie treffen können, informieren, z. B. den Einsatz spezieller ***Verschlüsselungssoftware*** oder ***anderer datenzentrierter Sicherheitstechnologien***.

Änderungsantrag 54

Vorschlag für eine Richtlinie
Erwägung 54

Vorschlag der Kommission	*Geänderter Text*
(54) Zur Aufrechterhaltung der Sicherheit elektronischer Kommunikationsnetze und -dienste sollte die Verschlüsselung, ***insbesondere von Ende zu Ende***, gefördert werden; erforderlichenfalls sollte sie für die Anbieter solcher Dienste und Netze im Einklang mit den Grundsätzen der Sicherheit und des Schutzes der Privatsphäre mittels datenschutzfreundlicher Voreinstellungen und Technikgestaltung für die Zwecke des Artikels 18 vorgeschrieben werden. Die Nutzung der End-zu-End-Verschlüsselung sollte mit den Befugnissen der Mitgliedstaaten, den Schutz ihrer wesentlichen Sicherheitsinteressen und der öffentlichen Sicherheit zu gewährleisten und die Ermittlung, Aufdeckung und Verfolgung von Straftaten im Einklang mit dem Unionsrecht zu ermöglichen, in Einklang gebracht werden. ***Lösungen für den rechtmäßigen Zugang*** zu ***Informationen in End-zu-End-verschlüsselter Kommunikation sollten*** die ***Wirksamkeit der Verschlüsselung beim Schutz der Privatsphäre*** und ***der Sicherheit*** der ***Kommunikation aufrechterhalten und zugleich eine wirksame Reaktion auf Straftaten gewährleisten***.	(54) Zur Aufrechterhaltung der Sicherheit elektronischer Kommunikationsnetze und -dienste sollte die Verschlüsselung ***und anderer datenzentrierter Sicherheitstechnologien***, ***wie Tokenisierung, Segmentierung, Zugriffsdrosselung, Markierung, Kennzeichnung, starkes Identitäts- und Zugriffsmanagement und automatische Zugriffsentscheidungen***, gefördert werden; erforderlichenfalls sollte sie für die Anbieter solcher Dienste und Netze im Einklang mit den Grundsätzen der Sicherheit und des Schutzes der Privatsphäre mittels datenschutzfreundlicher Voreinstellungen und Technikgestaltung für die Zwecke des Artikels 18 vorgeschrieben werden. Die Nutzung der End-zu-End-Verschlüsselung sollte mit den Befugnissen der Mitgliedstaaten, den Schutz ihrer wesentlichen Sicherheitsinteressen und der öffentlichen Sicherheit zu gewährleisten und die Ermittlung, Aufdeckung und Verfolgung von Straftaten im Einklang mit dem Unionsrecht zu ermöglichen, in Einklang gebracht werden. ***Dies sollte jedoch nicht*** zu ***einer Schwächung der End-zu-End-Verschlüsselung führen,*** die ***eine entscheidende Technologie für einen wirksamen Datenschutz*** und ***den Schutz*** der ***Privatsphäre ist***.

Änderungsantrag 55

Vorschlag für eine Richtlinie
Erwägung 54 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(54a) Um die Sicherheit zu gewährleisten und den Missbrauch und die Manipulation elektronischer Kommunikationsnetze und -dienste zu

verhindern, sollte die Verwendung interoperabler sicherer Routing-Standards gefördert werden, um die Integrität und Robustheit der Routing-Funktionen im gesamten Ökosystem der Internetbetreiber sicherzustellen.

Änderungsantrag 56

Vorschlag für eine Richtlinie
Erwägung 54 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	(54b) Um die Funktionalität und Integrität des Internets zu wahren und Sicherheitsprobleme im Zusammenhang mit dem DNS zu verringern, sollten die einschlägigen Akteure, einschließlich der Unternehmen in der Union, der Internet-Diensteanbieter und der Browser-Anbieter, dazu angehalten werden, eine Strategie zur Diversifizierung der DNS-Auflösung zu verfolgen. Außerdem sollten die Mitgliedstaaten die Entwicklung und Nutzung eines öffentlichen und sicheren europäischen DNS-Auflösungsdienstes fördern.

Änderungsantrag 57

Vorschlag für eine Richtlinie
Erwägung 55

Vorschlag der Kommission	*Geänderter Text*
(55) Mit dieser Richtlinie wird ein zweistufiger Ansatz für die Meldung von Sicherheitsvorfällen festgelegt, um die richtige Balance herzustellen zwischen einer zeitnahen Meldung einerseits, die einer potenziellen Ausbreitung von Sicherheitsvorfällen entgegenwirkt und den Einrichtungen die Möglichkeit gibt, Unterstützung zu erhalten, und einer detaillierten Meldung andererseits, bei der aus individuellen Sicherheitsvorfällen wichtige Lehren gezogen werden und	(55) Mit dieser Richtlinie wird ein zweistufiger Ansatz für die Meldung von Sicherheitsvorfällen festgelegt, um die richtige Balance herzustellen zwischen einer zeitnahen Meldung einerseits, die einer potenziellen Ausbreitung von Sicherheitsvorfällen entgegenwirkt und den Einrichtungen die Möglichkeit gibt, Unterstützung zu erhalten, und einer detaillierten Meldung andererseits, bei der aus individuellen Sicherheitsvorfällen wichtige Lehren gezogen werden und

einzelne Unternehmen und ganze Sektoren ihre Resilienz gegenüber Cyberbedrohungen im Laufe der Zeit verbessern können. Erhalten Einrichtungen Kenntnis von einem Sicherheitsvorfall, sollten sie innerhalb von ***24*** Stunden eine erste Meldung übermitteln und spätestens einen Monat ***danach einen Abschlussbericht vorlegen müssen. Die Erstmeldung sollte nur die Informationen enthalten, die unbedingt erforderlich sind, um die zuständigen Behörden über den Sicherheitsvorfall zu unterrichten und es*** der ***Einrichtung zu ermöglichen, bei Bedarf Hilfe in Anspruch zu nehmen. Gegebenenfalls sollte aus dieser Meldung hervorgehen, ob der Sicherheitsvorfall vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist. Die Mitgliedstaaten sollten sicherstellen, dass durch die Pflicht zur Übermittlung dieser Erstmeldung die Ressourcen*** der ***meldenden Einrichtung*** für ***Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen, die Vorrang haben sollten,*** nicht ***beeinträchtigt werden. Zur weiteren Verhinderung***, ***dass die Meldepflichten für Sicherheitsvorfälle entweder zulasten der Ressourcen gehen, auf solche Vorfälle*** zu ***reagieren***, ***oder entsprechende Anstrengungen der Einrichtungen anderweitig beeinträchtigt werden, sollten die Mitgliedstaaten auch vorsehen***, ***dass die betreffende Einrichtung in hinreichend begründeten Fällen*** und ***im Einvernehmen mit den zuständigen Behörden oder dem CSIRT von der Frist von 24 Stunden für*** die ***Erstmeldung bzw. einem Monat für den Abschlussbericht abweichen kann***.

einzelne Unternehmen und ganze Sektoren ihre Resilienz gegenüber Cyberbedrohungen im Laufe der Zeit verbessern können. Erhalten Einrichtungen Kenntnis von einem Sicherheitsvorfall, sollten sie innerhalb von ***72*** Stunden eine erste Meldung übermitteln und spätestens einen Monat ***nach*** der ***ersten*** Meldung ***einen umfassenden Bericht vorlegen müssen***. Der ***Zeitplan*** für ***die erste Meldung eines Sicherheitsvorfalls sollte Einrichtungen*** nicht ***daran hindern***, ***Vorfälle früher*** zu ***melden***, ***so dass sie rasch Unterstützung von CSIRTs anfordern können***, ***um den gemeldeten Sicherheitsvorfall einzudämmen*** und ***seine mögliche Ausbreitung zu verhindern. CSIRTs können einen Zwischenbericht über relevante Statusaktualisierungen anfordern und dabei*** die ***Reaktions- und Abhilfemaßnahmen der meldenden Einrichtung berücksichtigen***.

Änderungsantrag 58

Vorschlag für eine Richtlinie
Erwägung 55 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(55a) Ein erheblicher Sicherheitsvorfall kann Auswirkungen auf die Vertraulichkeit, Integrität oder Verfügbarkeit des Dienstes haben. Wesentliche und wichtige Einrichtungen sollten die CSIRTs innerhalb von 24 Stunden nach Bekanntwerden des Sicherheitsvorfalls über erhebliche Sicherheitsvorfälle informieren, die sich auf die Verfügbarkeit ihrer Dienste auswirken. Sie sollten die CIRTs innerhalb von 72 Stunden nach Bekanntwerden über erhebliche Sicherheitsvorfälle informieren, die die Vertraulichkeit und Integrität ihrer Dienste beeinträchtigen. Die Unterscheidung zwischen den Arten von Vorfällen beruht nicht auf der Schwere des Sicherheitsvorfalls, sondern darauf, wie schwierig es für die meldende Einrichtung ist, den Sicherheitsvorfall zu bewerten, seine Bedeutung einzuschätzen und Informationen zu melden, die für das CSIRT von Nutzen sein können. Die erste Meldung sollte die Informationen enthalten, die erforderlich sind, um das CSIRT über den Sicherheitsvorfall zu unterrichten und es der Einrichtung zu ermöglichen, bei Bedarf Hilfe in Anspruch zu nehmen. Die Mitgliedstaaten sollten sicherstellen, dass durch die Pflicht zur Übermittlung dieser Erstmeldung die Ressourcen der meldenden Einrichtung für Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen, die Vorrang haben sollten, nicht beeinträchtigt werden. Zur weiteren Verhinderung, dass die Meldepflichten für Sicherheitsvorfälle entweder zulasten der Ressourcen gehen, auf solche Vorfälle zu reagieren, oder entsprechende Anstrengungen der Einrichtungen anderweitig beeinträchtigt werden, sollten die Mitgliedstaaten auch vorsehen, dass die betreffende Einrichtung in hinreichend begründeten

Fällen und im Einvernehmen mit dem CSIRT von der Frist für die erste Meldung bzw. für den umfassenden Bericht abweichen kann.

Änderungsantrag 59

Vorschlag für eine Richtlinie
Erwägung 59

Vorschlag der Kommission	*Geänderter Text*
(59) Die Pflege genauer und vollständiger Datenbanken mit Domänennamen und Registrierungsdaten (sogenannte „WHOIS-Daten“) und ein rechtmäßiger Zugang zu diesen Daten sind entscheidend, um die Sicherheit, Stabilität und Resilienz des DNS zu gewährleisten, was wiederum zu einem hohen gemeinsamen Cybersicherheitsniveau in der Union beiträgt. Werden auch personenbezogene Daten verarbeitet, so muss diese Verarbeitung mit dem EU-Datenschutzrecht im Einklang stehen.	(59) Die Pflege genauer, überprüfter und vollständiger Datenbanken mit Domänennamen und Registrierungsdaten (sogenannte „WHOIS-Daten“) sind entscheidend, um die Sicherheit, Stabilität und Resilienz des DNS zu gewährleisten, was wiederum zu einem hohen gemeinsamen Cybersicherheitsniveau in der Union beiträgt, und um illegale Tätigkeiten zu bekämpfen. ***TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, sollten daher verpflichtet werden, Domänennamen-Registrierungsdaten zu erfassen, die zumindest den Namen der Registranten, ihre Anschrift, ihre E-Mail-Adresse und ihre Telefonnummer enthalten sollten. In der Praxis sind die gesammelten Daten möglicherweise nicht immer ganz genau, doch sollten TLD-Register und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, angemessene Verfahren einführen und umsetzen um zu überprüfen, ob natürliche oder juristische Personen, die einen Domänennamen beantragen oder besitzen, Kontaktdaten angegeben haben, unter denen sie erreichbar sind und bei deren Verwendung erwartet werden kann, dass sie antworten. Diese Überprüfungsverfahren sollten nach dem Konzept des „ihr Möglichstes tun“ die derzeit in der Branche verwendeten bewährten Verfahren widerspiegeln. Diese bewährten Verfahren im Überprüfungsprozess sollten den***

Fortschritten bei dem Prozess der elektronischen Identifizierung Rechnung tragen. Die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, sollten ihre Strategien und Verfahren zur Gewährleistung der Integrität und Verfügbarkeit der Domänennamen-Registrierungsdaten öffentlich zugänglich machen. Werden auch personenbezogene Daten verarbeitet, so muss diese Verarbeitung mit dem EU-Datenschutzrecht im Einklang stehen.

Änderungsantrag 60

Vorschlag für eine Richtlinie
Erwägung 60

Vorschlag der Kommission	*Geänderter Text*
(60) Die Verfügbarkeit und zeitnahe Zugänglichkeit dieser ***Daten*** für ***Behörden***, einschließlich der nach Unionsrecht oder nationalem Recht für die Verhütung, Ermittlung oder Verfolgung von Straftaten zuständigen Behörden***,*** CERTs***,*** CSIRTs ***und – soweit es*** die ***Daten ihrer Kunden betrifft – Anbietern elektronischer Kommunikationsnetze und -dienste sowie Anbietern*** von ***Cybersicherheitstechnologien*** und ***-diensten***, die ***im Namen dieser Kunden tätig sind***, ***ist*** von ***wesentlicher Bedeutung***, ***um Missbrauch des Domänennamensystems abzuwenden und zu bekämpfen und insbesondere Cybersicherheitsvorfällen vorzubeugen, sie zu erkennen*** und ***zu bewältigen***. ***Dieser Zugang sollte, soweit personenbezogene Daten betroffen sind, mit dem EU-Datenschutzrecht im Einklang stehen.***	(60) Die Verfügbarkeit und zeitnahe Zugänglichkeit dieser ***Domänennamen-Registrierungsdaten*** für ***berechtigte Zugangsnachfrager ist für die Cybersicherheit und die Bekämpfung illegaler Aktivitäten im Online-Ökosystem unerlässlich. TLD-Register und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, sollten daher verpflichtet werden, berechtigten Zugangsnachfragern im Einklang mit dem Datenschutzrecht der Union rechtmäßigen Zugang zu bestimmten Domänennamen-Registrierungsdaten, einschließlich personenbezogener Daten, zu gewähren. Berechtigte Zugangsnachfrager sollten einen hinreichend begründeten Antrag auf Zugang zu Domänennamen-Registrierungsdaten auf*** der ***Grundlage des Unionsrechts oder des nationalen Rechts stellen und könnten die*** nach Unionsrecht oder nationalem Recht für die Verhütung, Ermittlung oder Verfolgung von Straftaten zuständigen Behörden ***sowie nationale*** CERTs ***oder*** CSIRTs ***sein. Die Mitgliedstaaten sollten sicherstellen, dass TLD-Register und Stellen, die***

	Domänennamen-Registrierungsdienste erbringen, unverzüglich und in jedem Fall innerhalb von 72 Stunden auf Anträge von rechtmäßigen Antragstellern auf Offenlegung von Domänennamen-Registrierungsdaten reagieren sollten. TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, sollten Grundsätze und Verfahren für die Veröffentlichung und Offenlegung von Registrierungsdaten festlegen, einschließlich Leistungsvereinbarungen für die Bearbeitung von Anträgen berechtigter Zugangsnachfrager. Das Zugangsverfahren kann auch die Verwendung einer Schnittstelle, eines Portals oder anderer technischer Instrumente umfassen, um ein effizientes System für die Anforderung von und den Zugriff auf Registrierungsdaten bereitzustellen. Zur Förderung einheitlicher Verfahren für den gesamten Binnenmarkt kann die Kommission unbeschadet der Zuständigkeiten des Europäischen Datenschutzausschusses Leitlinien zu solchen Verfahren erlassen.

Änderungsantrag 61

Vorschlag für eine Richtlinie
Erwägung 61

Vorschlag der Kommission	*Geänderter Text*
(61) Zur Gewährleistung der Verfügbarkeit genauer und vollständiger Domänennamen-Registrierungsdaten sollten die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen (sogenannte Registrierstellen), die Integrität und Verfügbarkeit von Domänennamen-Registrierungsdaten erfassen und garantieren. Insbesondere sollten die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD	***entfällt***

erbringen, Grundsätze und Verfahren festlegen, um im Einklang mit den EU-Datenschutzvorschriften genaue und vollständige Registrierungsdaten zu erfassen und zu pflegen sowie unrichtige Registrierungsdaten zu verhindern bzw. zu berichtigen.

Änderungsantrag 62

Vorschlag für eine Richtlinie
Erwägung 62

Vorschlag der Kommission	*Geänderter Text*
(62) TLD-Register und ***die*** Einrichtungen, die Domänennamen-Registrierungsdienste ***für sie*** erbringen, sollten ***Domänennamen-Registrierungsdaten***, die ***nicht den EU-Datenschutzvorschriften unterliegen, z. B.*** Daten***, die juristische Personen betreffen[25]***, öffentlich zugänglich machen. ***TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, sollten*** es ***auch ermöglichen, dass berechtigte Zugangsnachfrager rechtmäßigen Zugang zu bestimmten Domänennamen-Registrierungsdaten natürlicher*** Personen ***im Einklang mit dem EU-Datenschutzrecht erhalten. Die Mitgliedstaaten sollten sicherstellen***, ***dass TLD-Register*** und ***die Einrichtungen, die Domänennamen-Registrierungsdienste für sie erbringen, Anträge berechtigter Zugangsnachfrager auf Offenlegung*** von ***Domänennamen-Registrierungsdaten unverzüglich beantworten. TLD-Register und die Einrichtungen***, ***die Domänennamen-Registrierungsdienste für*** sie ***erbringen, sollten Grundsätze und Verfahren für*** die ***Veröffentlichung und Offenlegung von Registrierungsdaten festlegen***, ***einschließlich Leistungsvereinbarungen für die Bearbeitung von Anträgen berechtigter Zugangsnachfrager***. ***Das Zugangsverfahren kann auch die***	(62) TLD-Register und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, sollten ***verpflichtet werden***, die ***Registrierungsdaten, die keine personenbezogenen*** Daten ***enthalten***, öffentlich zugänglich ***zu*** machen. Es ***sollte zwischen natürlichen und juristischen Personen unterschieden werden[25]. Bei juristischen*** Personen ***sollten TLD-Register und Einrichtungen zumindest den Namen des Registranten***, ***seine physische*** und ***seine E-Mail-Adresse sowie seine Telefonnummer öffentlich zugänglich machen.*** Von ***der juristischen Person sollte verlangt werden***, ***dass*** sie ***entweder eine allgemeine E-Mail-Adresse angibt,*** die ***öffentlich zugänglich gemacht werden kann***, ***oder dass sie der Veröffentlichung einer persönlichen E-Mail-Adresse zustimmt***. ***Die juristische Person sollte in der Lage sein***, ***diese Zustimmung auf Anforderung durch TLD-Register und Einrichtungen***, die ***Domänennamen-Registrierungsdienste erbringen, nachzuweisen***.

Verwendung einer Schnittstelle, eines Portals oder eines anderen technischen Instruments umfassen, um ein effizientes System für die Anforderung von und den Zugriff auf Registrierungsdaten bereitzustellen. Zur Förderung einheitlicher Verfahren für den gesamten Binnenmarkt kann die Kommission unbeschadet der Zuständigkeiten des Europäischen Datenschutzausschusses Leitlinien zu solchen Verfahren erlassen.

---

[25] Erwägungsgrund 14 der VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES: „Diese Verordnung gilt nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person."

---

[25] Erwägungsgrund 14 der VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES: „Diese Verordnung gilt nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person."

Änderungsantrag 63

Vorschlag für eine Richtlinie
Erwägung 63

Vorschlag der Kommission	*Geänderter Text*
(63) Alle wesentlichen und wichtigen Einrichtungen, die unter diese Richtlinie fallen, sollten der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegen, in dem sie ihre Dienste erbringen. Erbringt die Einrichtung Dienste in mehreren Mitgliedstaaten, so sollte sie unter die getrennte und parallele gerichtliche Zuständigkeit der betreffenden Mitgliedstaaten fallen. Die zuständigen Behörden dieser Mitgliedstaaten sollten zusammenarbeiten, einander Amtshilfe leisten und gegebenenfalls gemeinsame Aufsichtstätigkeiten durchführen.	(63) Alle wesentlichen und wichtigen Einrichtungen, die unter diese Richtlinie fallen, sollten der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegen, in dem sie ihre Dienste erbringen ***oder ihre Tätigkeiten ausüben***. Erbringt die Einrichtung Dienste in mehreren Mitgliedstaaten, so sollte sie unter die getrennte und parallele gerichtliche Zuständigkeit der betreffenden Mitgliedstaaten fallen. Die zuständigen Behörden dieser Mitgliedstaaten sollten zusammenarbeiten, einander Amtshilfe leisten und gegebenenfalls gemeinsame Aufsichtstätigkeiten durchführen.

Änderungsantrag 64

Vorschlag für eine Richtlinie
Erwägung 64

Vorschlag der Kommission	*Geänderter Text*
(64) Da die Dienste und Tätigkeiten, die von DNS-Diensteanbietern, TLD-Namenregistern, Betreibern von Inhaltszustellnetzen, Anbietern von Cloud-Computing-Diensten sowie Anbietern von Rechenzentrumsdiensten und Anbietern digitaler Dienste erbracht werden, grenzübergreifenden Charakter haben, sollte jeweils immer nur ein Mitgliedstaat für diese Einrichtungen zuständig sein. Die gerichtliche Zuständigkeit sollte bei dem Mitgliedstaat liegen, in dem die betreffende Einrichtung ihre Hauptniederlassung in der Union hat. Das Kriterium der Niederlassung im Sinne dieser Richtlinie setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei unerheblich. Dieses Kriterium sollte nicht davon abhängen, ob die Netz- und Informationssysteme an einem bestimmten Ort physisch untergebracht sind; die Existenz und die Nutzung derartiger Systeme stellen an sich keine derartige Hauptniederlassung dar und sind daher kein ausschlaggebendes Kriterium für die Bestimmung der Hauptniederlassung. Die Hauptniederlassung sollte der Ort sein, an dem in der Union über Maßnahmen des Cybersicherheitsrisikomanagements entschieden wird. In der Regel entspricht dies dem Ort, an dem sich die Hauptverwaltung der Unternehmen in der Union befindet. Werden solche Entscheidungen nicht in der Union getroffen, sollte davon ausgegangen werden, dass sich die Hauptniederlassung in dem Mitgliedstaat ***befindet***, in dem die	(64) Da die Dienste und Tätigkeiten, die von DNS-Diensteanbietern, TLD-Namenregistern, Betreibern von Inhaltszustellnetzen, Anbietern von Cloud-Computing-Diensten sowie Anbietern von Rechenzentrumsdiensten und Anbietern digitaler Dienste erbracht werden, grenzübergreifenden Charakter haben, sollte jeweils immer nur ein Mitgliedstaat für diese Einrichtungen zuständig sein. Die gerichtliche Zuständigkeit sollte bei dem Mitgliedstaat liegen, in dem die betreffende Einrichtung ihre Hauptniederlassung in der Union hat. Das Kriterium der Niederlassung im Sinne dieser Richtlinie setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei unerheblich. Dieses Kriterium sollte nicht davon abhängen, ob die Netz- und Informationssysteme an einem bestimmten Ort physisch untergebracht sind; die Existenz und die Nutzung derartiger Systeme stellen an sich keine derartige Hauptniederlassung dar und sind daher kein ausschlaggebendes Kriterium für die Bestimmung der Hauptniederlassung. Die Hauptniederlassung sollte der Ort sein, an dem in der Union über Maßnahmen des Cybersicherheitsrisikomanagements entschieden wird. In der Regel entspricht dies dem Ort, an dem sich die Hauptverwaltung der Unternehmen in der Union befindet. Werden solche Entscheidungen nicht in der Union getroffen, sollte davon ausgegangen werden, dass sich die Hauptniederlassung ***entweder*** in dem Mitgliedstaat, in dem die

Einrichtung über ***eine*** Niederlassung mit der unionsweit höchsten Beschäftigtenzahl verfügt. Werden die Dienste von einer Unternehmensgruppe ausgeführt, so sollte die Hauptniederlassung des herrschenden Unternehmens als Hauptniederlassung der Unternehmensgruppe gelten.	Einrichtung über ***die*** Niederlassung mit der unionsweit höchsten Beschäftigtenzahl verfügt***, oder in dem Mitgliedstaat befindet, in dem die Niederlassung liegt, in der die Cybersicherheits-Operationen ausgeführt werden***. Werden die Dienste von einer Unternehmensgruppe ausgeführt, so sollte die Hauptniederlassung des herrschenden Unternehmens als Hauptniederlassung der Unternehmensgruppe gelten.

Änderungsantrag 65

Vorschlag für eine Richtlinie
Erwägung 65 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(65a) Die ENISA sollte ein Register einrichten und führen, das Informationen über wesentliche und wichtige Einrichtungen enthält sowie DNS-Dienstanbieter, TLD-Namensregistrierungsstellen und Anbieter von Cloud-Computing-Diensten, Rechenzentrumsdiensten, Inhaltsbereitstellungsnetzwerke, Online-Marktplätze, Online-Suchmaschinen und Plattformen für soziale Netzwerke umfasst. Diese wesentlichen und wichtigen Einrichtungen sollten der ENISA ihre Namen, Adressen und aktuellen Kontaktdaten übermitteln. Sie sollten ENISA unverzüglich und in jedem Fall innerhalb von zwei Wochen ab dem Zeitpunkt des Inkrafttretens der Änderung über alle Änderungen dieser Angaben informieren. Die ENISA sollte die Informationen an die zuständige zentrale Anlaufstelle weiterleiten. Die wesentlichen und wichtigen Einrichtungen, die ihre Informationen an die ENISA übermitteln, sind daher nicht verpflichtet, die zuständige Behörde des Mitgliedstaates gesondert zu informieren. Die ENISA könnte ein einfaches, öffentlich zugängliches Anwendungsprogramm entwickeln, das

	diese Einrichtungen zur Aktualisierung ihrer Informationen nutzen können. Außerdem sollte die ENISA geeignete Informationsklassifizierungs- und -verwaltungsprotokolle erstellen, um die Sicherheit und Vertraulichkeit offengelegter Informationen sicherzustellen und den Zugang, die Speicherung und die Übermittlung derartiger Informationen an die vorgesehenen Nutzer zu beschränken.

Änderungsantrag 66

Vorschlag für eine Richtlinie
Erwägung 66

Vorschlag der Kommission	*Geänderter Text*
(66) Werden nach nationalem Recht oder Unionsrecht als Verschlusssache geltende Informationen gemäß den Bestimmungen dieser Richtlinie ausgetauscht, gemeldet oder auf andere Weise weitergegeben, so sollten die entsprechenden besonderen Vorschriften für den Umgang mit Verschlusssachen angewandt werden.	(66) Werden nach nationalem Recht oder Unionsrecht als Verschlusssache geltende Informationen gemäß den Bestimmungen dieser Richtlinie ausgetauscht, gemeldet oder auf andere Weise weitergegeben, so sollten die entsprechenden besonderen Vorschriften für den Umgang mit Verschlusssachen angewandt werden. ***Darüber hinaus sollte die ENISA über die Infrastruktur, Verfahren und Vorschriften verfügen, um sensible und als Verschlusssache eingestufte Informationen im Einklang mit den geltenden Sicherheitsvorschriften zum Schutz von EU-Verschlusssachen zu behandeln.***

Änderungsantrag 67

Vorschlag für eine Richtlinie
Erwägung 68

Vorschlag der Kommission	*Geänderter Text*
(68) Die Einrichtungen sollten ermutigt werden, ihre individuellen Kenntnisse und praktischen Erfahrungen auf strategischer, taktischer und operativer Ebene gemeinsam zu nutzen, damit sich ihre	(68) Die Einrichtungen sollten ermutigt ***und von den Mitgliedstaaten dabei unterstützt*** werden, ihre individuellen Kenntnisse und praktischen Erfahrungen auf strategischer, taktischer und operativer

Fähigkeit verbessert, Cyberbedrohungen angemessen zu bewerten, zu überwachen***,*** abzuwehren und auf sie zu reagieren. Daher muss dafür gesorgt werden, dass auf Unionsebene Mechanismen für Vereinbarungen über den freiwilligen Informationsaustausch entstehen können. Zu diesem Zweck sollten die Mitgliedstaaten auch einschlägige Einrichtungen, die nicht unter diese Richtlinie fallen, aktiv unterstützen und dazu anhalten, sich an solchen Mechanismen zum Informationsaustausch zu beteiligen. Diese Mechanismen sollten unter uneingeschränkter Einhaltung der Wettbewerbsvorschriften und des Datenschutzrechts der Union eingerichtet werden.

Ebene gemeinsam zu nutzen, damit sich ihre Fähigkeit verbessert, Cyberbedrohungen angemessen zu bewerten, zu überwachen ***und*** abzuwehren und auf sie zu reagieren. Daher muss dafür gesorgt werden, dass auf Unionsebene Mechanismen für Vereinbarungen über den freiwilligen Informationsaustausch entstehen können. Zu diesem Zweck sollten die Mitgliedstaaten auch einschlägige Einrichtungen, die nicht unter diese Richtlinie fallen***, wie Einrichtungen, die sich auf Cybersicherheitsdienstleistungen und -forschung konzentrieren***, aktiv unterstützen und dazu anhalten, sich an solchen Mechanismen zum Informationsaustausch zu beteiligen. Diese Mechanismen sollten unter uneingeschränkter Einhaltung der Wettbewerbsvorschriften und des Datenschutzrechts der Union eingerichtet werden.

Änderungsantrag 68

Vorschlag für eine Richtlinie
Erwägung 69

Vorschlag der Kommission	*Geänderter Text*
(69) Die Verarbeitung personenbezogener Daten durch ***Einrichtungen, Behörden, CERTs***, CSIRTs sowie Anbieter von Sicherheitstechnologien und -diensten ***sollte im Sinne*** der Verordnung (EU) 2016/679 ***ein berechtigtes Interesse des jeweiligen Verantwortlichen darstellen, wie dies für*** die ***Gewährleistung*** der ***Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist. Dies sollte auch Folgendes einschließen:*** Maßnahmen im Hinblick auf die Verhütung, Erkennung, Analyse und Bewältigung von Sicherheitsvorfällen, Maßnahmen zur Sensibilisierung für spezifische Cyberbedrohungen,	(69) Die Verarbeitung personenbezogener Daten durch ***wesentliche und wichtige Einrichtungen***, CSIRTs sowie Anbieter von Sicherheitstechnologien und -diensten***, ist für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig, und ist für die Erfüllung ihrer rechtlichen Verpflichtungen gemäß dieser Richtlinie erforderlich; eine solche Verarbeitung personenbezogener Daten kann auch für die Zwecke der von wesentlichen und wichtigen Einrichtungen verfolgten berechtigten Interessen erforderlich sein. Erfordert diese Richtlinie die Verarbeitung personenbezogener Daten zum Zwecke der Cybersicherheit und der***

Informationsaustausch im Zusammenhang mit der Behebung von Schwachstellen und ihrer koordinierten Offenlegung, freiwilliger Austausch von Informationen über solche Sicherheitsvorfälle sowie über Cyberbedrohungen und Schwachstellen, Gefährdungsindikatoren, Taktiken, Vorgehensweisen und Verfahren, Cybersicherheitswarnungen und Konfigurationstools***. Diese Maßnahmen können*** die Verarbeitung ***folgender Arten*** personenbezogener Daten ***erfordern:*** IP-Adressen, Uniform Resource Locators (URL-Adressen), Domänennamen ***und E-Mail-Adressen***.	***Netz- und Informationssicherheit gemäß den Bestimmungen der Artikel 18, 20 und 23 der Richtlinie, gilt diese Verarbeitung als zur Erfüllung einer rechtlichen Verpflichtung erforderlich gemäß Artikel 6 Absatz 1 Buchstabe c*** der Verordnung (EU) 2016/679***. Für die Zwecke der Artikel 26 und 27 dieser Richtlinie gilt die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 als erforderlich für die Zwecke der berechtigten Interessen, die von den wesentlichen und wichtigen Einrichtungen verfolgt werden.*** Maßnahmen im Hinblick auf die Verhütung, Erkennung***, Identifizierung, Eindämmung***, Analyse und Bewältigung von Sicherheitsvorfällen, Maßnahmen zur Sensibilisierung für spezifische Cyberbedrohungen, Informationsaustausch im Zusammenhang mit der Behebung von Schwachstellen und ihrer koordinierten Offenlegung, freiwilliger Austausch von Informationen über solche Sicherheitsvorfälle sowie über Cyberbedrohungen und Schwachstellen, Gefährdungsindikatoren, Taktiken, Vorgehensweisen und Verfahren, Cybersicherheitswarnungen und Konfigurationstools ***erfordern*** die Verarbeitung ***bestimmter Kategorien*** personenbezogener Daten ***wie*** IP-Adressen, Uniform Resource Locators (URL-Adressen), Domänennamen***, E-Mail-Adressen, Zeitstempel, betriebssystem- oder browserbezogener Informationen oder anderer Informationen, die auf den Modus Operandi hinweisen***.

Änderungsantrag 69

Vorschlag für eine Richtlinie
Erwägung 71

Vorschlag der Kommission	*Geänderter Text*
(71) Für eine wirksame Durchsetzung sollte ein Mindestumfang von	(71) Für eine wirksame Durchsetzung sollte ein Mindestumfang von

Verwaltungssanktionen für Verstöße gegen die Verpflichtungen im Bereich des Cybersicherheitsrisikomanagements und die Meldepflichten gemäß dieser Richtlinie festgelegt werden, womit für die gesamte Union ein klarer und kohärenter Rahmen für solche Sanktionen geschaffen wird. Folgendem sollte gebührend Rechnung getragen werden: der Art, Schwere und Dauer des Verstoßes, den ***tatsächlich*** entstandenen Schäden oder Verlusten ***bzw. den Schäden oder Verlusten, die hätten entstehen können***, der Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, den Maßnahmen zur Vermeidung oder Minderung der entstandenen Schäden/Verluste, dem Grad der Verantwortlichkeit oder jeglichem früheren Verstoß, dem Umfang der Zusammenarbeit mit der Aufsichtsbehörde sowie jedem anderen erschwerenden oder mildernden Umstand. Für die Verhängung von Sanktionen einschließlich Geldbußen sollte es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta der Grundrechte der Europäischen Union, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, entsprechen.

Verwaltungssanktionen für Verstöße gegen die Verpflichtungen im Bereich des Cybersicherheitsrisikomanagements und die Meldepflichten gemäß dieser Richtlinie festgelegt werden, womit für die gesamte Union ein klarer und kohärenter Rahmen für solche Sanktionen geschaffen wird. Folgendem sollte gebührend Rechnung getragen werden: der Art, Schwere und Dauer des Verstoßes, den entstandenen Schäden oder Verlusten, der Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, den Maßnahmen zur Vermeidung oder Minderung der entstandenen Schäden/Verluste, dem Grad der Verantwortlichkeit oder jeglichem früheren Verstoß, dem Umfang der Zusammenarbeit mit der Aufsichtsbehörde sowie jedem anderen erschwerenden oder mildernden Umstand. Für die Verhängung von Sanktionen einschließlich Geldbußen***, die verhältnismäßig sein sollten,*** sollte es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta der Grundrechte der Europäischen Union ***(die „Charta“)***, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren ***sowie der Unschuldsvermutung und der Verteidigungsrechte***, entsprechen.

Änderungsantrag 70

Vorschlag für eine Richtlinie
Erwägung 72

Vorschlag der Kommission	*Geänderter Text*
(72) Um die wirksame Durchsetzung der in dieser Richtlinie festgelegten Verpflichtungen zu gewährleisten, sollte jede zuständige Behörde befugt sein, Geldbußen aufzuerlegen oder ihre Auferlegung zu beantragen.	(72) Um die wirksame Durchsetzung der in dieser Richtlinie festgelegten Verpflichtungen zu gewährleisten, sollte jede zuständige Behörde befugt sein, Geldbußen aufzuerlegen oder ihre Auferlegung zu beantragen***, wenn die Zuwiderhandlung vorsätzlich oder fahrlässig war oder die Einrichtung zuvor darüber informiert worden ist, dass die Einrichtung eine Zuwiderhandlung***

begeht.

Änderungsantrag 71

Vorschlag für eine Richtlinie
Erwägung 76

Vorschlag der Kommission	*Geänderter Text*
(76) Um die Wirksamkeit und Abschreckungskraft der Sanktionen bei Verstößen gegen die Verpflichtungen aus dieser Richtlinie zu erhöhen, sollten die zuständigen Behörden befugt sein, ***Sanktionen zu verhängen, die darin bestehen, die*** Zertifizierung oder Genehmigung für einen Teil oder alle von einer wesentlichen Einrichtung erbrachten Dienste ***auszusetzen*** und natürlichen Personen die Ausübung von Leitungsaufgaben vorübergehend ***zu untersagen***. Angesichts ihrer Schwere und ihrer Auswirkungen auf die Tätigkeiten der Einrichtungen und letztlich auf ihre Verbraucher sollten solche ***Sanktionen*** im Verhältnis zur Schwere des Verstoßes und unter Berücksichtigung der besonderen Umstände des Einzelfalls verhängt werden; hierzu zählen auch die Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, sowie die zur Verhinderung oder Minderung des erlittenen Schadens und/oder der erlittenen Verluste ergriffenen Maßnahmen. ***Solche Sanktionen*** sollten nur als äußerstes Mittel verhängt werden, also erst nachdem die anderen einschlägigen Durchsetzungsmaßnahmen nach dieser Richtlinie ausgeschöpft wurden, und nur so lange, bis die betroffenen Einrichtungen die erforderlichen Maßnahmen zur Behebung der Mängel ergreifen oder die Anforderungen der zuständigen Behörde, auf die sich die ***Sanktionen*** beziehen, erfüllen. Für die ***Verhängung*** solcher ***Sanktionen*** muss es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta ***der Grundrechte der***	(76) Um die Wirksamkeit und Abschreckungskraft der Sanktionen bei Verstößen gegen die Verpflichtungen aus dieser Richtlinie zu erhöhen, sollten die zuständigen Behörden befugt sein, ***eine vorübergehende Aussetzung der*** Zertifizierung oder Genehmigung für einen Teil oder alle von einer wesentlichen Einrichtung erbrachten ***relevanten*** Dienste ***anzuwenden,*** und ***zu verlangen, dass*** natürlichen Personen die Ausübung von Leitungsaufgaben ***auf Geschäftsführungs- bzw. Vorstandsebene oder Ebene des rechtlichen Vertreters*** vorübergehend ***untersagt wird. Die Mitgliedstaaten sollten spezifische Verfahren und Vorschriften für das vorübergehende Verbot der Ausübung von Leitungsaufgaben durch eine natürliche Person auf Geschäftsführungs- bzw. Vorstandsebene oder Ebene des rechtlichen Vertreters in Einrichtungen der öffentlichen Verwaltung entwickeln. Bei der Ausarbeitung solcher Verfahren und Vorschriften sollten die Mitgliedstaaten die Besonderheiten ihrer jeweiligen Verwaltungsebenen und -systeme innerhalb ihrer öffentlichen Verwaltungen berücksichtigen.*** Angesichts ihrer Schwere und ihrer Auswirkungen auf die Tätigkeiten der Einrichtungen und letztlich auf ihre Verbraucher sollten solche ***vorübergehenden Aussetzungen oder Verbote*** im Verhältnis zur Schwere des Verstoßes und unter Berücksichtigung der besonderen Umstände des Einzelfalls verhängt werden; hierzu zählen auch die Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, sowie die zur

Europäischen Union, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, der Unschuldsvermutung und des Rechts auf Verteidigung, entsprechen.

Verhinderung oder Minderung des erlittenen Schadens und/oder der erlittenen Verluste ergriffenen Maßnahmen. ***Vorübergehende Aussetzungen oder Verbote*** sollten nur als äußerstes Mittel verhängt werden, also erst nachdem die anderen einschlägigen Durchsetzungsmaßnahmen nach dieser Richtlinie ausgeschöpft wurden, und nur so lange, bis die betroffenen Einrichtungen die erforderlichen Maßnahmen zur Behebung der Mängel ergreifen oder die Anforderungen der zuständigen Behörde, auf die sich die ***vorübergehenden Aussetzungen oder Verbote*** beziehen, erfüllen. Für die ***Anwendung*** solcher ***vorübergehenden Aussetzungen oder Verbote*** muss es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, der Unschuldsvermutung und des Rechts auf Verteidigung, entsprechen.

Änderungsantrag 72

Vorschlag für eine Richtlinie
Erwägung 79

Vorschlag der Kommission	*Geänderter Text*
(79) Es sollte ein Peer-Review-Mechanismus eingeführt werden, der es ermöglicht, dass von den Mitgliedstaaten benannte Sachverständige die Umsetzung der Cybersicherheitsstrategien, einschließlich der Kapazitäten der Mitgliedstaaten und der verfügbaren Ressourcen, einer Bewertung unterziehen.	(79) Es sollte ein Peer-Review-Mechanismus eingeführt werden, der es ermöglicht, dass von den Mitgliedstaaten benannte unabhängige Sachverständige die Umsetzung der Cybersicherheitsstrategien, einschließlich der Kapazitäten der Mitgliedstaaten und der verfügbaren Ressourcen, einer Bewertung unterziehen. ***Peer-Reviews können zu wertvollen Erkenntnissen und Empfehlungen führen, die die allgemeinen Cybersicherheitsfähigkeiten stärken. Sie können insbesondere dazu beitragen, den Transfer von Technologien, Werkzeugen, Maßnahmen und Verfahren zwischen den an der Peer-Review beteiligten Mitgliedstaaten zu erleichtern, einen***

funktionalen Weg für den Austausch bewährter Verfahren zwischen Mitgliedstaaten mit unterschiedlichem Reifegrad im Bereich der Cybersicherheit zu schaffen und die Erreichung eines hohen, gemeinsamen Cybersicherheitsniveaus in der gesamten Union zu ermöglichen. Der Peer-Review sollte eine Selbstbewertung des zu überprüfenden Mitgliedstaats vorausgehen, die sich auf die überprüften Aspekte und alle zusätzlichen gezielten Fragen erstreckt, die die benannten Sachverständigen dem zu überprüfenden Mitgliedstaat vor Beginn des Verfahrens mitteilen. Die Kommission sollte in Zusammenarbeit mit der ENISA und der Kooperationsgruppe Vorlagen für die Selbstbewertung der überprüften Aspekte entwickeln, um den Prozess zu straffen und verfahrenstechnische Unstimmigkeiten und Verzögerungen zu vermeiden, die die einer Peer-Review unterzogenen Mitgliedstaaten ausfüllen und den benannten Sachverständigen, die die Peer-Review durchführen, vor Beginn des Peer-Review-Verfahrens übermitteln sollten.

Änderungsantrag 73

Vorschlag für eine Richtlinie
Erwägung 80

Vorschlag der Kommission	*Geänderter Text*
(80) Um neuen Cyberbedrohungen, technologischen Entwicklungen oder sektorspezifischen Eigenschaften Rechnung zu tragen, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte in Bezug auf Elemente zu erlassen, die die in dieser Richtlinie vorgeschriebenen Risikomanagementmaßnahmen betreffen. Der Kommission sollte auch die Befugnis übertragen werden, delegierte Rechtsakte zu erlassen, in denen festgelegt wird,	(80) Um neuen Cyberbedrohungen, technologischen Entwicklungen oder sektorspezifischen Eigenschaften Rechnung zu tragen, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte in Bezug auf Elemente zu erlassen, die die in dieser Richtlinie vorgeschriebenen Risikomanagementmaßnahmen ***und Meldepflichten im Bereich der Cybersicherheit*** betreffen. Der Kommission sollte auch die Befugnis

welche Kategorien wesentlicher Einrichtungen ein Zertifikat erlangen müssen und welche spezifischen europäischen Schemata für die Cybersicherheitszertifizierung dabei anzuwenden sind. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung[26] niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, 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 Vorbereitung der delegierten Rechtsakte befasst sind.

übertragen werden, delegierte Rechtsakte zu erlassen, in denen festgelegt wird, welche Kategorien wesentlicher ***und wichtigen*** Einrichtungen ein Zertifikat erlangen müssen und welche spezifischen europäischen Schemata für die Cybersicherheitszertifizierung dabei anzuwenden sind. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, 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 Vorbereitung der delegierten Rechtsakte befasst sind.

---

[26] ABl. L 123 vom 12.5.2016, S. 1.

Änderungsantrag 74

Vorschlag für eine Richtlinie
Erwägung 81

Vorschlag der Kommission	*Geänderter Text*
(81) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung der einschlägigen Bestimmungen dieser Richtlinie in Bezug auf die Verfahrensmodalitäten, die für das Funktionieren der Kooperationsgruppe erforderlich sind, ***die technischen Elemente im Zusammenhang mit Risikomanagementmaßnahmen oder die Art der Informationen, das Format und*** das Verfahren für die Meldung von Sicherheitsvorfällen, sollten der	(81) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung der einschlägigen Bestimmungen dieser Richtlinie in Bezug auf die Verfahrensmodalitäten, die für das Funktionieren der Kooperationsgruppe erforderlich sind, das Verfahren für die Meldung von Sicherheitsvorfällen, sollten der Kommission Durchführungsbefugnisse übertragen werden. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen

Kommission Durchführungsbefugnisse übertragen werden. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates[27] ausgeübt werden.

Parlaments und des Rates[27] ausgeübt werden.

---

[27] 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).

[27] 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).

Änderungsantrag 75

Vorschlag für eine Richtlinie
Erwägung 82

Vorschlag der Kommission	*Geänderter Text*
(82) Die Kommission sollte diese Richtlinie regelmäßig in Abstimmung mit interessierten Kreisen überprüfen, insbesondere um festzustellen, ob ***sie veränderten gesellschaftlichen***, ***politischen*** oder ***technischen*** Bedingungen oder ***veränderten*** Marktbedingungen ***anzupassen*** ist.	(82) Die Kommission sollte diese Richtlinie regelmäßig in Abstimmung mit interessierten Kreisen überprüfen, insbesondere um festzustellen, ob ***angesichts veränderter gesellschaftlicher***, ***politischer*** oder ***technischer*** Bedingungen oder ***veränderter*** Marktbedingungen ***Änderungen vorgeschlagen werden sollten. Im Rahmen dieser Überprüfungen sollte die Kommission die Bedeutung der in den Anhängen genannten Sektoren, Teilsektoren und Arten von Einrichtungen für das Funktionieren von Wirtschaft und Gesellschaft in Bezug auf die Cybersicherheit bewerten. Die Kommission sollte unter anderem prüfen, ob digitale Anbieter, die als sehr große Online-Plattformen im Sinne von Artikel 25 der Verordnung (EU) XXXX/XXXX [Binnenmarkt für digitale Dienstleistungen (Gesetz über digitale Dienstleistungen)] oder als Gatekeeper im Sinne von Artikel 2 Nummer 1 der***

***Verordnung (EU) XXXX/XXXX [Bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte)] eingestuft werden, als wesentliche Einrichtungen im Sinne dieser Richtlinie benannt werden sollten. Darüber hinaus sollte die Kommission prüfen, ob es angemessen* ist*, Anhang I der Richtlinie 2020/1828 des Europäischen Parlaments und des Rates[1a] zu ändern und einen Verweis auf die vorliegende Richtlinie hinzuzufügen*.

_____

1a Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates vom 25. November 2020 über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher und zur Aufhebung der Richtlinie 2009/22/EG (ABl. L 409 vom 4.12.2020, S. 1).

Änderungsantrag 76
Vorschlag für eine Richtlinie
Erwägung 82 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(82a) Durch diese Richtlinie werden die Anforderungen an die Cybersicherheit für die Mitgliedstaaten sowie für wesentliche und wichtige Einrichtungen mit Sitz in der Union festgelegt. Diese Anforderungen an die Cybersicherheit sollten auch von den Organen, Einrichtungen und sonstigen Stellen der Union auf der Grundlage eines Rechtsakts der Union angewandt werden.

Änderungsantrag 77

Vorschlag für eine Richtlinie
Erwägung 82 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	(82b) Mit dieser Richtlinie werden neue Aufgaben für die ENISA geschaffen, wodurch ihre Rolle gestärkt wird, und sie könnte auch dazu führen, dass die ENISA ihre bestehenden Aufgaben gemäß der Verordnung (EU) 2019/881 auf einem höheren Niveau als zuvor ausführen muss. Um sicherzustellen, dass die ENISA über die erforderlichen finanziellen und personellen Ressourcen verfügt, um bestehende und neue Tätigkeiten im Rahmen ihrer Aufgaben durchzuführen und um etwaigen höheren Anforderungen, die sich aus ihrer erweiterten Rolle ergeben, gerecht zu werden, sollte ihr Haushalt entsprechend aufgestockt werden. Um eine effiziente Nutzung der Ressourcen zu gewährleisten, sollte die ENISA außerdem eine größere Flexibilität bei der Art und Weise erhalten, in der es ihr gestattet ist, die Ressourcen intern zuzuweisen, damit sie in der Lage ist, ihre Aufgaben effektiv wahrzunehmen und die Erwartungen zu erfüllen.

Änderungsantrag 78

Vorschlag für eine Richtlinie
Erwägung 84

Vorschlag der Kommission	*Geänderter Text*
(84) Diese Richtlinie steht mit den in der Charta ***der Grundrechte der Europäischen Union*** anerkannten Grundrechten und Grundsätzen, insbesondere der Achtung des Privatlebens und der Kommunikation, dem Schutz personenbezogener Daten, der unternehmerischen Freiheit, dem Eigentumsrecht, dem Recht auf einen wirksamen Rechtsbehelf und dem Recht, gehört zu werden, im Einklang. Diese Richtlinie sollte im Einklang mit diesen Rechten und Grundsätzen umgesetzt	(84) Diese Richtlinie steht mit den in der Charta anerkannten Grundrechten und Grundsätzen, insbesondere der Achtung des Privatlebens und der Kommunikation, dem Schutz personenbezogener Daten, der unternehmerischen Freiheit, dem Eigentumsrecht, dem Recht auf einen wirksamen Rechtsbehelf und dem Recht, gehört zu werden, im Einklang. ***Dazu gehört auch das Recht auf einen wirksamen Rechtsbehelf vor einem Gericht für die Empfänger von Dienstleistungen, die von wesentlichen***

werden ——	***und wichtigen Einrichtungen erbracht werden.*** Diese Richtlinie sollte im Einklang mit diesen Rechten und Grundsätzen umgesetzt werden***.***

Änderungsantrag 79

Vorschlag für eine Richtlinie
Artikel 1 – Absatz 2 – Buchstabe c a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ca) Aufsichts- und Durchsetzungspflichten für die Mitgliedstaaten.

Änderungsantrag 80

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Diese Richtlinie gilt für öffentliche und private Einrichtungen der in Anhang I als wesentliche Einrichtungen und in Anhang II als wichtige Einrichtungen aufgeführten Arten. Diese Richtlinie gilt nicht für ***Einrichtungen, die als Kleinstunternehmen*** und ***kleine Unternehmen im Sinne*** der Empfehlung 2003/361/EG der Kommission[28] ***angesehen werden***.	(1) Diese Richtlinie gilt für öffentliche und private ***wesentliche und wichtige*** Einrichtungen der in Anhang I als wesentliche Einrichtungen und in Anhang II als wichtige Einrichtungen aufgeführten Arten***, die ihre Dienstleistungen innerhalb der Union erbringen oder ihre Tätigkeiten dort ausüben***. Diese Richtlinie gilt nicht für ***Kleinst- oder Kleinunternehmen im Sinne von Artikel 2 Absätze 2*** und ***3 des Anhangs*** der Empfehlung 2003/361/EG der Kommission[28]***. Artikel 3 Absatz 4 des Anhangs der Empfehlung ist nicht anwendbar.***
[28] Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).	[28] Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).

Änderungsantrag 81

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 2 – Unterabsatz 1 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
Unabhängig von der Größe der Einrichtungen gilt diese Richtlinie ***jedoch*** auch für ***die in den Anhängen I*** und ***II genannten*** Einrichtungen, wenn	Unabhängig von der Größe der Einrichtungen gilt diese Richtlinie auch für ***wesentliche*** und ***wichtige*** Einrichtungen, wenn

Änderungsantrag 82

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 2 – Unterabsatz 1 – Buchstabe d

Vorschlag der Kommission	*Geänderter Text*
d) sich eine ***mögliche*** Störung des von der Einrichtung erbrachten Dienstes auf die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken könnte;	d) sich eine Störung des von der Einrichtung erbrachten Dienstes auf die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken könnte;

Änderungsantrag 83

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 2 - Unterabsatz 1 – Buchstabe e

Vorschlag der Kommission	*Geänderter Text*
e) eine ***mögliche*** Störung des von der Einrichtung erbrachten Dienstes zu Systemrisiken führen könnte, insbesondere in Sektoren, in denen eine solche Störung grenzübergreifende Auswirkungen haben könnte;	e) eine Störung des von der Einrichtung erbrachten Dienstes zu Systemrisiken führen könnte, insbesondere in Sektoren, in denen eine solche Störung grenzübergreifende Auswirkungen haben könnte;

Änderungsantrag 84

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 2 – Unterabsatz 2

Vorschlag der Kommission	*Geänderter Text*
Die Mitgliedstaaten erstellen eine Liste der gemäß den Buchstaben b bis f	***entfällt***

ermittelten Einrichtungen und übermitteln sie der Kommission bis zum [6 Monate nach Ablauf der Umsetzungsfrist]. Danach überprüfen die Mitgliedstaaten die Liste regelmäßig und mindestens alle zwei Jahre und aktualisieren sie gegebenenfalls.

Änderungsantrag 85

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 2 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(2a) Bis zum ... [6 Monate nach Ablauf der Umsetzungsfrist] erstellen die Mitgliedstaaten eine Liste der wesentlichen und wichtigen Einrichtungen, einschließlich der in Absatz 1 genannten Einrichtungen und der gemäß Absatz 2 Buchstaben b bis f und Artikel 24 Absatz 1 ermittelten Einrichtungen. Die Mitgliedstaaten überprüfen diese Liste danach regelmäßig, mindestens jedoch alle zwei Jahre, und aktualisieren sie gegebenenfalls.

Änderungsantrag 86

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 2 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	(2b) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen den zuständigen Behörden zumindest die folgenden Informationen übermitteln:
	a) Name der Einrichtung,
	b) Anschrift und aktuelle Kontaktdaten, einschließlich E-Mail-Adressen, IP-Bereiche, Telefonnummern, sowie
	c) relevante(n) Sektor(en) und

Teilsektor(en) gemäß den Anhängen I und II.

Die wesentlichen und wichtigen Einrichtungen teilen alle Änderungen der gemäß Unterabsatz 1 übermittelten Angaben unverzüglich mit, in jedem Fall jedoch innerhalb von zwei Wochen ab dem Zeitpunkt, an dem die Änderung wirksam wird. Zu diesem Zweck gibt die Kommission mit Unterstützung der ENISA unverzüglich Leitlinien und Vorlagen für die in diesem Absatz genannten Verpflichtungen heraus.

Änderungsantrag 87

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 2 c (neu)

Vorschlag der Kommission	*Geänderter Text*
	(2c) Bis zum ... [6 Monate nach Ablauf der Umsetzungsfrist] und danach alle zwei Jahre melden die Mitgliedstaaten
	a) der Kommission und der Kooperationsgruppe die Anzahl aller wesentlichen und wichtigen Einrichtungen, die für jeden Sektor und Teilsektor gemäß den Anhängen I und II ermittelt wurden, und
	b) der Kommission die Namen der gemäß Absatz 2 Buchstaben b bis f ermittelten Einrichtungen.

Änderungsantrag 88

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
(4) Diese Richtlinie gilt unbeschadet der Richtlinie 2008/114/EG des Rates[30] ***sowie*** der Richtlinien 2011/93/EU[31] und ***2013/40***/EU***[32]*** des Europäischen Parlaments und des Rates.	(4) Diese Richtlinie gilt unbeschadet der Richtlinie 2008/114/EG des Rates[30] ***und*** der Richtlinien 2011/93/EU[31] und ***2002/58***/EU des Europäischen Parlaments und des Rates***[32a]***.

[30] Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern (ABl. L 345 vom 23.12.2008, S. 75).

[31] Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates (ABl. L 335 vom 17.12.2011, S. 1).

[32] Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates (ABl. L 218 vom 14.8.2013, S. 8).

[30] Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern (ABl. L 345 vom 23.12.2008, S. 75).

[31] Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates (ABl. L 335 vom 17.12.2011, S. 1).

[32] Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates (ABl. L 218 vom 14.8.2013, S. 8).

32a Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

Änderungsantrag 89

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
(6) Wenn wesentliche oder wichtige Einrichtungen gemäß den Bestimmungen sektorspezifischer Rechtsakte der Union entweder Maßnahmen zum Cybersicherheitsrisikomanagement ergreifen oder Sicherheitsvorfälle und erhebliche Cyberbedrohungen melden müssen und wenn die entsprechenden Anforderungen in ihrer Wirkung den in dieser Richtlinie festgelegten	(6) Wenn wesentliche oder wichtige Einrichtungen gemäß den Bestimmungen sektorspezifischer Rechtsakte der Union Maßnahmen zum Cybersicherheitsrisikomanagement ergreifen oder Sicherheitsvorfälle melden müssen und wenn die entsprechenden Anforderungen in ihrer Wirkung den in dieser Richtlinie festgelegten Verpflichtungen, auch den in Kapitel VI

Verpflichtungen, auch den in Kapitel VI festgelegten Bestimmungen in Bezug auf die Aufsicht und die Durchsetzung, zumindest gleichwertig sind, finden die einschlägigen Bestimmungen dieser Richtlinie keine Anwendung.	festgelegten Bestimmungen in Bezug auf die Aufsicht und die Durchsetzung, zumindest gleichwertig sind, finden die einschlägigen Bestimmungen dieser Richtlinie keine Anwendung. ***Die Kommission erlässt unverzüglich Leitlinien für die Durchführung der sektorspezifischen Rechtsakte der Union um sicherzustellen, dass die in dieser Richtlinie festgelegten Anforderungen an die Cybersicherheit durch diese Rechtsakte erfüllt werden und dass es nicht zu Überschneidungen oder Rechtsunsicherheit kommt. Bei der Ausarbeitung dieser Leitlinien trägt die Kommission den bewährten Verfahren und dem Fachwissen der ENISA und der Kooperationsgruppe Rechnung.***

Änderungsantrag 90

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 6 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(6a) Wesentliche und wichtige Einrichtungen, CSIRTs und Anbieter von Sicherheitstechnologien und -diensten verarbeiten personenbezogene Daten, soweit dies für die Zwecke der Cybersicherheit sowie der Netz- und Informationssicherheit unbedingt erforderlich und verhältnismäßig ist, um die in dieser Richtlinie festgelegten Verpflichtungen zu erfüllen. Diese Verarbeitung personenbezogener Daten nach dieser Richtlinie erfolgt im Einklang mit der Verordnung (EU) 2016/679, insbesondere mit ihrem Artikel 6.

Änderungsantrag 91

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 6 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	(6b) Die Verarbeitung personenbezogener Daten gemäß dieser Richtlinie durch Anbieter öffentlicher elektronischer Kommunikationsnetze oder Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste gemäß Anhang I Nummer 8 erfolgt im Einklang mit der Richtlinie 2002/58/EG.

Änderungsantrag 92

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 4 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(4a) „Beinahe-Vorfall“ ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten hätte gefährden können oder einen Schaden hätte verursachen können, dessen negative Auswirkungen jedoch erfolgreich verhindert wurden;

Änderungsantrag 93

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 6

Vorschlag der Kommission	*Geänderter Text*
6. „Bewältigung von Sicherheitsvorfällen“ alle Maßnahmen und Verfahren zur Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen sowie die Reaktion darauf;	6. „Bewältigung von Sicherheitsvorfällen“ alle Maßnahmen und Verfahren zur ***Verhütung,*** Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen sowie die Reaktion darauf;

Änderungsantrag 94

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 7a (neu)

Vorschlag der Kommission	*Geänderter Text*
	7a. „Risiko“ das Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall verursacht werden, das als eine Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens dieses Sicherheitsvorfalls zum Ausdruck gebracht wird;

Änderungsantrag 95

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 11

Vorschlag der Kommission	*Geänderter Text*
11. „technische Spezifikation“ eine technische Spezifikation im Sinne des Artikels 2 Nummer ***4*** der Verordnung (EU) Nr. ***1025/2012***;	11. „technische Spezifikation“ eine technische Spezifikation im Sinne des Artikels 2 Nummer ***20*** der Verordnung (EU) Nr. ***2019/881***;

Änderungsantrag 96

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 13

Vorschlag der Kommission	*Geänderter Text*
13. „Domänennamensystem (DNS)“ ein verteiltes hierarchisches Verzeichnissystem, das ***es den Endnutzern ermöglicht, Dienste*** und Ressourcen im Internet zu erreichen;	13. „Domänennamensystem“ (DNS) ein verteiltes hierarchisches Verzeichnissystem, das ***die Identifizierung von Diensten*** und Ressourcen im Internet ***ermöglicht und es Endnutzergeräten erlaubt, Internet-Routing- und Konnektivitätsdienste zu nutzen, um diese Dienste und Ressourcen*** zu erreichen;

Änderungsantrag 97

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 14

Vorschlag der Kommission	*Geänderter Text*
14. „DNS-Diensteanbieter“ eine	14. „DNS-Diensteanbieter“ eine

Einrichtung, die ***Internet-Endnutzern und anderen DNS-Diensteanbietern rekursive oder autoritative Dienste zur Auflösung von Domänennamen anbietet;***	Einrichtung, die

Änderungsantrag 98

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 14 – Buchstabe a (neu)

Vorschlag der Kommission	*Geänderter Text*
	a) Internet-Endnutzern offene oder öffentliche rekursive Dienste zur Auflösung von Domänennamen anbietet oder

Änderungsantrag 99

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 14 – Buchstabe b (neu)

Vorschlag der Kommission	*Geänderter Text*
	b) autoritative Dienste zur Auflösung von Domänennamen als Dienstleistung, die von Drittanbietern bezogen werden kann, anbietet;

Änderungsantrag 100

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 15

Vorschlag der Kommission	*Geänderter Text*
15. „Namenregister der Domäne oberster Stufe“ (TLD-Register) eine Einrichtung, der eine bestimmte Domäne oberster Stufe (Top Level Domain – TLD) übertragen wurde und die für die Verwaltung der TLD, einschließlich der Registrierung von Domänennamen unterhalb der TLD, sowie für den technischen Betrieb der TLD, einschließlich des Betriebs ihrer Namenserver, der Pflege ihrer Datenbanken und der Verteilung von TLD-	15. „Namenregister der Domäne oberster Stufe“ (TLD-Register) eine Einrichtung, der eine bestimmte Domäne oberster Stufe (Top Level Domain – TLD) übertragen wurde und die für die Verwaltung der TLD, einschließlich der Registrierung von Domänennamen unterhalb der TLD, sowie für den technischen Betrieb der TLD, einschließlich des Betriebs ihrer Namenserver, der Pflege ihrer Datenbanken und der Verteilung von TLD-

Zonendateien über die Namenserver, zuständig ist;	Zonendateien über die Namenserver, zuständig ist***, unabhängig davon, ob der Betrieb durch eine Einrichtung oder extern erfolgt***;

Änderungsantrag 101

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 15 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	15a. „Domänennamen-Registrierungsdienste“ Dienste, die von Domänennamen-Registern und Domänennamen-Registrierungsstellen, Anbietern von Datenschutz- oder Proxy-Registrierungsdiensten, Domänenmaklern oder Wiederverkäufern erbracht werden, sowie alle anderen Dienste, die mit der Registrierung von Domänennamen zusammenhängen;

Änderungsantrag 102

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 23 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	23a. „öffentliches elektronisches Kommunikationsnetz“ ein öffentliches elektronisches Kommunikationsnetz im Sinne von Artikel 2 Nummer 8 der Richtlinie (EU) 2018/1972;

Änderungsantrag 103

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 23 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	23b. „elektronischer Kommunikationsdienste“ elektronische Kommunikationsdienste im Sinne des Artikels 2 Nummer 4 der Richtlinie (EU) 2018/1972;

Änderungsantrag 104

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 1 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(1) Jeder Mitgliedstaat ***verabschiedet*** eine nationale Cybersicherheitsstrategie, in der die strategischen Ziele sowie angemessene politische und regulatorische Maßnahmen zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus festgelegt werden. Die nationale Cybersicherheitsstrategie muss insbesondere Folgendes umfassen:	(1) Jeder Mitgliedstaat ***nimmt*** eine nationale Cybersicherheitsstrategie ***an***, in der die strategischen ***Ziele, die erforderlichen technischen, organisatorischen und finanziellen Ressourcen zur Erreichung dieser*** Ziele sowie angemessene politische und regulatorische Maßnahmen zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus festgelegt werden. Die nationale Cybersicherheitsstrategie muss insbesondere Folgendes umfassen:

Änderungsantrag 105

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 1 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) eine Beschreibung der für die Cybersicherheitsstrategie des ***jeweiligen*** Mitgliedstaats festgelegten Ziele und Prioritäten;	a) eine Beschreibung der für die Cybersicherheitsstrategie des Mitgliedstaats festgelegten Ziele und Prioritäten;

Änderungsantrag 106

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 1 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) einen Steuerungsrahmen zur Verwirklichung dieser Ziele und Prioritäten, der die in Absatz 2 genannten Konzepte ***sowie die Aufgaben und Zuständigkeiten öffentlicher Stellen und Einrichtungen sowie anderer relevanter Akteure umfasst***;	b) einen Steuerungsrahmen zur Verwirklichung dieser Ziele und Prioritäten, der die in Absatz 2 genannten Konzepte;

Änderungsantrag 107

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 1 – Buchstabe b a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ba) einen Rahmen, in dem die Aufgaben und Zuständigkeiten der öffentlichen Stellen und Einrichtungen sowie anderer einschlägiger Akteure festgelegt werden und der die Zusammenarbeit und Koordinierung auf nationaler Ebene zwischen den gemäß Artikel 7 Absatz 1 und Artikel 8 Absatz 1 benannten zuständigen Behörden, der gemäß Artikel 8 Absatz 3 benannten zentralen Anlaufstelle und den gemäß Artikel 9 benannten CSIRTs unterstützt;

Änderungsantrag 108

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 1 – Buchstabe e

Vorschlag der Kommission	*Geänderter Text*
e) eine Liste der verschiedenen Behörden und Akteure, die an der Umsetzung der nationalen Cybersicherheitsstrategie beteiligt sind;	e) eine Liste der verschiedenen Behörden und Akteure, die an der Umsetzung der nationalen Cybersicherheitsstrategie beteiligt sind***, einschließlich einer zentralen Anlaufstelle für die Cybersicherheit für KMU, die Unterstützung bei der Umsetzung der spezifischen Cybersicherheitsmaßnahmen bietet***;

Änderungsantrag 109

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 1 – Buchstabe f

Vorschlag der Kommission	*Geänderter Text*
f) einen politischen Rahmen für eine verstärkte Koordinierung zwischen den zuständigen Behörden im Rahmen dieser Richtlinie und der Richtlinie (EU) XXXX/XXXX des Europäischen	f) einen politischen Rahmen für eine verstärkte Koordinierung zwischen den zuständigen Behörden im Rahmen dieser Richtlinie und der Richtlinie (EU)XXXX/XXXX des Europäischen

Parlaments und des Rates[38] [Richtlinie über die Resilienz kritischer Einrichtungen] für die Zwecke des Informationsaustauschs über Sicherheitsvorfälle und Cyberbedrohungen und der Wahrnehmung von Aufsichtsaufgaben.	Parlaments und des Rates [Richtlinie über die Resilienz kritischer Einrichtungen][38] ***, sowohl in als auch zwischen den Mitgliedstaaten,*** für die Zwecke des Informationsaustauschs über Sicherheitsvorfälle und Cyberbedrohungen und der Wahrnehmung von Aufsichtsaufgaben.
[38] [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].	[38] [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].

Änderungsantrag 110

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 1 – Buchstabe f a (neu)

Vorschlag der Kommission	*Geänderter Text*
	fa) eine Bewertung des allgemeinen Bewusstseins für Cybersicherheit bei den Bürgerinnen und Bürgern.

Änderungsantrag 111

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe -a (neu)

Vorschlag der Kommission	*Geänderter Text*
	-a) ein Konzept für die Cybersicherheit für jeden Sektor, der durch diese Richtlinie geregelt wird;

Änderungsantrag 112

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) Leitlinien für die Aufnahme und Spezifikation cybersicherheitsbezogener Anforderungen an IKT-Produkte und -Dienste bei der Vergabe öffentlicher Aufträge;	b) Leitlinien für die Aufnahme und Spezifikation cybersicherheitsbezogener Anforderungen an IKT-Produkte und -Dienste bei der Vergabe öffentlicher Aufträge***, einschließlich Verschlüsselungsanforderungen und der***

	Nutzung quelloffener Cybersicherheitsprodukte;

Änderungsantrag 113

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe d

Vorschlag der Kommission	*Geänderter Text*
d) ein Konzept im Zusammenhang mit der Aufrechterhaltung der allgemeinen Verfügbarkeit und Integrität des öffentlichen Kerns des offenen Internets;	d) ein Konzept im Zusammenhang mit der Aufrechterhaltung der allgemeinen Verfügbarkeit und Integrität des öffentlichen Kerns des offenen Internets***, einschließlich der Cybersicherheit von Unterseekommunikationskabeln***;

Änderungsantrag 114

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe d a (neu)

Vorschlag der Kommission	*Geänderter Text*
	da) ein Konzept zur Förderung und Unterstützung der Entwicklung und Integration sich abzeichnender Technologien wie künstliche Intelligenz bei Tools und Anwendungen zur Verbesserung der Cybersicherheit;

Änderungsantrag 115

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe d b (neu)

Vorschlag der Kommission	*Geänderter Text*
	db) ein Konzept zur Förderung der Integration von Open-Source-Tools und -Anwendungen;

Änderungsantrag 116

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe f

Vorschlag der Kommission	*Geänderter Text*
f) ein Konzept zur Unterstützung von Hochschul- und Forschungseinrichtungen bei der Entwicklung von Cybersicherheitsinstrumenten und sicherer Netzinfrastruktur;	f) ein Konzept zur Unterstützung von Hochschul- und Forschungseinrichtungen bei der Entwicklung***, der Verbesserung und des Einsatzes*** von Cybersicherheitsinstrumenten und sicherer Netzinfrastruktur;

Änderungsantrag 117

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe h

Vorschlag der Kommission	*Geänderter Text*
h) ein Konzept***, das auf die spezifischen Bedürfnisse von*** KMU – ***insbesondere*** vom Anwendungsbereich dieser Richtlinie ausgenommener KMU – ***ausgerichtet ist*** und Orientierungshilfen sowie Unterstützung ***bei*** der ***Verbesserung ihrer Resilienz gegenüber Cybersicherheitsbedrohungen bietet.***	h) ein Konzept ***zur Förderung der Cybersicherheit für*** KMU***,*** – ***einschließlich*** vom Anwendungsbereich dieser Richtlinie ausgenommener KMU – ***das auf ihre besonderen Bedürfnisse eingeht*** und Orientierungshilfen sowie Unterstützung ***bietet, einschließlich Leitlinien für die Bewältigung*** der ***aufgetretenen Herausforderungen in der Lieferkette;***

Änderungsantrag 118

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe h a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ha) ein Konzept zur Förderung der Cyber-Hygiene, das ein Basispaket von Praktiken und Kontrollen umfasst, sowie eine allgemeine Sensibilisierung der Bürger für Cyber-Sicherheitsbedrohungen und bewährte Verfahren;

Änderungsantrag 119

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe h b (neu)

Vorschlag der Kommission	*Geänderter Text*
	hb) ein Konzept zur Förderung der aktiven Cyberverteidigung

Änderungsantrag 120

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe h c (neu)

Vorschlag der Kommission	*Geänderter Text*
	hc) ein Konzept, das den Behörden dabei hilft, Kompetenzen zu entwickeln und Verständnis für die Sicherheitsüberlegungen zu schaffen, die für die Planung, den Bau und die Verwaltung vernetzter Orte erforderlich sind.

Änderungsantrag 121

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe h d (neu)

Vorschlag der Kommission	*Geänderter Text*
	hd) ein Konzept, das sich speziell mit der Bedrohung durch Ransomware befasst und das Ransomware-Geschäftsmodell stört;

Änderungsantrag 122

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe h e (neu)

Vorschlag der Kommission	*Geänderter Text*
	he) ein Konzept, einschließlich einschlägiger Verfahren und Steuerungsrahmen, um die Einrichtung von ÖPPs für die Cybersicherheit zu unterstützen und zu fördern;

Änderungsantrag 123

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Die Mitgliedstaaten notifizieren der Kommission ihre nationalen Cybersicherheitsstrategien innerhalb von drei Monaten nach ihrer Verabschiedung. Die Mitgliedstaaten können bestimmte Informationen von der Notifizierung ausnehmen, wenn und soweit dies zur Wahrung der nationalen Sicherheit ***unbedingt*** erforderlich ist.	(3) Die Mitgliedstaaten notifizieren der Kommission ihre nationalen Cybersicherheitsstrategien innerhalb von drei Monaten nach ihrer Verabschiedung. Die Mitgliedstaaten können bestimmte Informationen von der Notifizierung ausnehmen, wenn und soweit dies zur Wahrung der nationalen Sicherheit erforderlich ist.

Änderungsantrag 124

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
(4) Die Mitgliedstaaten bewerten ihre nationalen Cybersicherheitsstrategien mindestens alle vier Jahre auf der Grundlage wesentlicher Leistungsindikatoren und ändern diese erforderlichenfalls. Die Agentur der Europäischen Union für Cybersicherheit (ENISA) unterstützt die Mitgliedstaaten auf Anfrage bei der Entwicklung einer nationalen Strategie und wesentlicher Leistungsindikatoren für die Bewertung der Strategie.	(4) Die Mitgliedstaaten bewerten ihre nationalen Cybersicherheitsstrategien mindestens alle vier Jahre auf der Grundlage wesentlicher Leistungsindikatoren und ändern diese erforderlichenfalls. Die Agentur der Europäischen Union für Cybersicherheit (ENISA) unterstützt die Mitgliedstaaten auf Anfrage bei der Entwicklung einer nationalen Strategie und wesentlicher Leistungsindikatoren für die Bewertung der Strategie. ***Die ENISA stellt den Mitgliedstaaten Leitlinien zur Verfügung, um ihre bereits formulierten nationalen Cybersicherheitsstrategien an die in dieser Richtlinie festgelegten Anforderungen und Verpflichtungen anzupassen.***

Änderungsantrag 125

Vorschlag für eine Richtlinie
Artikel 6 – Überschrift

Vorschlag der Kommission	*Geänderter Text*
Koordinierte Offenlegung von Schwachstellen und ***europäisches Schwachstellenregister***	Koordinierte Offenlegung von Schwachstellen und ***eine europäische Schwachstellendatenbank***

Änderungsantrag 126

Vorschlag für eine Richtlinie
Artikel 6 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Jeder Mitgliedstaat benennt eines seiner CSIRTs gemäß Artikel 9 als Koordinator für die Zwecke einer koordinierten Offenlegung von Schwachstellen. Das benannte CSIRT fungiert als vertrauenswürdiger Vermittler und erleichtert ***erforderlichenfalls*** die Interaktion zwischen der meldenden Einrichtung und dem Hersteller oder Anbieter von IKT-Produkten oder -Diensten. Betrifft die gemeldete Schwachstelle mehrere Hersteller oder Anbieter von IKT-Produkten oder -Diensten in der Union, so arbeitet das benannte CSIRT jedes betroffenen Mitgliedstaats mit dem CSIRT-Netzwerk zusammen.	(1) Jeder Mitgliedstaat benennt eines seiner CSIRTs gemäß Artikel 9 als Koordinator für die Zwecke einer koordinierten Offenlegung von Schwachstellen. Das benannte CSIRT fungiert als vertrauenswürdiger Vermittler und erleichtert ***auf Ersuchen der meldenden Einrichtung*** die Interaktion zwischen der meldenden Einrichtung und dem Hersteller oder Anbieter von IKT-Produkten oder -Diensten. Betrifft die gemeldete Schwachstelle mehrere Hersteller oder Anbieter von IKT-Produkten oder -Diensten in der Union, so arbeitet das benannte CSIRT jedes betroffenen Mitgliedstaats mit dem CSIRT-Netzwerk zusammen.

Änderungsantrag 127

Vorschlag für eine Richtlinie
Artikel 6 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die ENISA entwickelt und pflegt ***ein europäisches Schwachstellenregister***. Zu diesem Zweck führt die ENISA geeignete Informationssysteme, Konzepte und Verfahren ein ***und*** pflegt diese, damit insbesondere wichtige und wesentliche Einrichtungen ***sowie*** deren Anbieter von Netz- und Informationssystemen Schwachstellen in IKT-Produkten oder -	(2) Die ENISA entwickelt und pflegt ***eine europäische Schwachstellendatenbank, bei der das globale Common Vulnerabilities and Exposures (CVE – Bekannte Schwachstellen und Anfälligkeiten) zum Einsatz kommt***. Zu diesem Zweck führt die ENISA geeignete Informationssysteme, Konzepte und Verfahren ein**,** pflegt diese

Diensten offenlegen und registrieren können ***und*** allen interessierten Kreisen Zugang zu den ***im Register*** enthaltenen Informationen über Schwachstellen gewährt ***werden kann. Das Register muss insbesondere Folgendes umfassen:*** Informationen zur Beschreibung der Schwachstelle, des betroffenen IKT-Produkts oder der betroffenen IKT-Dienste sowie zum Ausmaß der Schwachstelle im Hinblick auf die Umstände, unter denen sie ausgenutzt werden kann, Informationen zur Verfügbarkeit entsprechender Patches ***und*** bei Nichtverfügbarkeit von Patches Orientierungshilfen für die Nutzer gefährdeter ***Produkte*** und ***Dienste***, wie die von offengelegten Schwachstellen ausgehenden Risiken gemindert werden können.

und trifft die erforderlichen technischen und organisatorischen Maßnahmen, um die Sicherheit und Integrität der Datenbank zu gewährleisten, damit insbesondere wichtige und wesentliche Einrichtungen ***und*** deren Anbieter von Netz- und Informationssystemen ***sowie Einrichtungen, die nicht in den Anwendungsbereich dieser Richtlinie fallen,*** Schwachstellen in IKT-Produkten oder -Diensten offenlegen und registrieren können***.*** Allen interessierten Kreisen ***wird*** Zugang zu den ***in der Datenbank*** enthaltenen Informationen über Schwachstellen gewährt***, für die Patches oder Abhilfemaßnahmen verfügbar sind.*** Informationen zur Beschreibung der Schwachstelle, des betroffenen IKT-Produkts oder der betroffenen IKT-Dienste sowie zum Ausmaß der Schwachstelle im Hinblick auf die Umstände, unter denen sie ausgenutzt werden kann, Informationen zur Verfügbarkeit entsprechender Patches Bei Nichtverfügbarkeit von Patches ***werden*** Orientierungshilfen für die Nutzer gefährdeter ***IKT-Produkte*** und ***-Dienste***, wie die von offengelegten Schwachstellen ausgehenden Risiken gemindert werden können***, in die Datenbank aufgenommen***.

Änderungsantrag 128

Vorschlag für eine Richtlinie
Artikel 7 – Absatz 1 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(1a) Benennt ein Mitgliedstaat mehr als eine zuständige Behörde im Sinne von Absatz 1, gibt er eindeutig an, welche dieser zuständigen Behörden als Koordinator für das Management von Sicherheitsvorfällen großen Ausmaßes und Krisen fungiert.

Änderungsantrag 129

Vorschlag für eine Richtlinie
Artikel 7 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Jeder Mitgliedstaat ermittelt die Kapazitäten, Mittel und Verfahren, die im ***Krisenfall*** für die Zwecke dieser Richtlinie eingesetzt werden können.	(2) Jeder Mitgliedstaat ermittelt die Kapazitäten, Mittel und Verfahren, die im ***Fall einer Krise*** für die Zwecke dieser Richtlinie eingesetzt werden können.

Änderungsantrag 130

Vorschlag für eine Richtlinie
Artikel 7 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
(4) Die Mitgliedstaaten teilen der Kommission ihre gemäß Absatz 1 benannten zuständigen Behörden innerhalb von drei Monaten nach der Benennung mit und übermitteln ihre nationalen Pläne für die Reaktion auf Cybersicherheitsvorfälle und -krisen gemäß Absatz 3 innerhalb von drei Monaten nach der Verabschiedung dieser Pläne. Die Mitgliedstaaten können bestimmte Informationen von ihrem Plan ausnehmen, wenn und soweit dies für ihre nationale Sicherheit unbedingt erforderlich ist.	(4) Die Mitgliedstaaten teilen der Kommission ihre gemäß Absatz 1 benannten zuständigen Behörden innerhalb von drei Monaten nach der Benennung mit und übermitteln ***dem EU-CyCLONe*** ihre nationalen Pläne für die Reaktion auf Cybersicherheitsvorfälle und -krisen gemäß Absatz 3 innerhalb von drei Monaten nach der Verabschiedung dieser Pläne. Die Mitgliedstaaten können bestimmte Informationen von ihrem Plan ausnehmen, wenn und soweit dies für ihre nationale Sicherheit unbedingt erforderlich ist.

Änderungsantrag 131

Vorschlag für eine Richtlinie
Artikel 8 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Jeder Mitgliedstaat benennt eine für die Cybersicherheit zuständige nationale zentrale Anlaufstelle (im Folgenden „zentrale Anlaufstelle“). Benennt ein Mitgliedstaat nur eine zuständige Behörde, so ist diese zuständige Behörde auch die zentrale Anlaufstelle dieses Mitgliedstaats.	(3) Jeder Mitgliedstaat benennt eine ***der gemäß Absatz 1 benannten zuständigen Behörden als eine*** für die Cybersicherheit zuständige nationale zentrale Anlaufstelle (im Folgenden „zentrale Anlaufstelle“). Benennt ein Mitgliedstaat nur eine zuständige Behörde, so ist diese zuständige Behörde auch die zentrale Anlaufstelle dieses Mitgliedstaats.

Änderungsantrag 132

Vorschlag für eine Richtlinie
Artikel 8 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
(4) Jede zentrale Anlaufstelle fungiert als Verbindungsstelle, um die grenzüberschreitende Zusammenarbeit der Behörden des Mitgliedstaats mit den entsprechenden Behörden in anderen Mitgliedstaaten sowie die sektorübergreifende Zusammenarbeit mit anderen nationalen zuständigen Behörden innerhalb des Mitgliedstaats zu gewährleisten.	(4) Jede zentrale Anlaufstelle fungiert als Verbindungsstelle, um die grenzüberschreitende Zusammenarbeit der Behörden des Mitgliedstaats mit den entsprechenden Behörden in anderen Mitgliedstaaten***, der Kommission und ENISA*** sowie die sektorübergreifende Zusammenarbeit mit anderen nationalen zuständigen Behörden innerhalb des Mitgliedstaats zu gewährleisten.

Änderungsantrag 133

Vorschlag für eine Richtlinie
Artikel 9 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Mitgliedstaaten gewährleisten, dass jedes CSIRT mit angemessenen Ressourcen ausgestattet ist, damit es seine in Artikel 10 Absatz 2 aufgeführten Aufgaben wirksam erfüllen kann.	(2) Die Mitgliedstaaten gewährleisten, dass jedes CSIRT mit angemessenen Ressourcen ausgestattet ist ***und über die notwendigen technischen Fähigkeiten verfügt***, damit es seine in Artikel 10 Absatz 2 aufgeführten Aufgaben wirksam erfüllen kann.

Änderungsantrag 134

Vorschlag für eine Richtlinie
Artikel 9 – Absatz 6 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(6a) Die Mitgliedstaaten gewährleisten die Möglichkeit eines wirksamen, effizienten und sicheren Informationsaustauschs auf allen Geheimhaltungsstufen zwischen ihren eigenen CSIRTs und CSIRTs aus Drittländern auf derselben Geheimhaltungsstufe.

Änderungsantrag 135

Vorschlag für eine Richtlinie
Artikel 9 – Absatz 6 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	(6b) Unbeschadet des Unionsrechts, insbesondere der Verordnung (EU) 2016/679, arbeiten die CSIRTs mit den CSIRTs oder gleichwertigen Einrichtungen in den Kandidatenländern und in anderen Drittländern des westlichen Balkans und der Östlichen Partnerschaft zusammen und leisten ihnen nach Möglichkeit Unterstützung im Bereich der Cybersicherheit.

Änderungsantrag 136

Vorschlag für eine Richtlinie
Artikel 9 – Absatz 7

Vorschlag der Kommission	*Geänderter Text*
(7) Die Mitgliedstaaten teilen der Kommission unverzüglich die gemäß Absatz 1 benannten CSIRTs**,** das gemäß Artikel 6 Absatz 1 als Koordinator benannte CSIRT ***und*** deren jeweilige in Bezug auf die ***in den Anhängen I*** und ***II genannten*** Einrichtungen vorgesehenen Aufgaben mit.	(7) Die Mitgliedstaaten teilen der Kommission unverzüglich die gemäß Absatz 1 benannten CSIRTs ***und*** das gemäß Artikel 6 Absatz 1 als Koordinator benannte CSIRT***, einschließlich*** deren jeweilige in Bezug auf die ***wesentlichen*** und ***wichtigen*** Einrichtungen vorgesehenen Aufgaben**,** mit.

Änderungsantrag 137

Vorschlag für eine Richtlinie
Artikel 10 – Überschrift

Vorschlag der Kommission	*Geänderter Text*
Anforderungen an die CSIRTs und Aufgaben der CSIRTs	Anforderungen an die CSIRTs ***sowie technische Kapazitäten*** und Aufgaben der CSIRTs

Änderungsantrag 138

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 1 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) Die CSIRTs müssen über ein geeignetes System zur ***Verwaltung und*** Weiterleitung von Anfragen verfügen, insbesondere, um wirksame und effiziente Übergaben zu erleichtern;	c) Die CSIRTs müssen über ein geeignetes System zur ***Klassifizierung,*** Weiterleitung ***und Nachverfolgung*** von Anfragen verfügen, insbesondere, um wirksame und effiziente Übergaben zu erleichtern;

Änderungsantrag 139

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 1 – Buchstabe c a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ca) Die CSIRTs verfügen über geeignete Verhaltenskodizes, um die Vertraulichkeit und Vertrauenswürdigkeit ihrer Tätigkeiten sicherzustellen;

Änderungsantrag 140

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 1 – Buchstabe d

Vorschlag der Kommission	*Geänderter Text*
d) Die CSIRTs müssen personell so ausgestattet sein, dass sie eine ständige Bereitschaft gewährleisten können;	d) Die CSIRTs müssen personell so ausgestattet sein, dass sie eine ständige Bereitschaft gewährleisten können***, und müssen einen angemessenen Schulungsrahmen für ihr Personal sicherstellen***;

Änderungsantrag 141

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 1 – Buchstabe e

Vorschlag der Kommission	*Geänderter Text*
e) Die CSIRTs müssen über Redundanzsysteme und Ausweicharbeitsräume verfügen, um die	e) Die CSIRTs müssen über Redundanzsysteme und Ausweicharbeitsräume verfügen, um die

Kontinuität ihrer Dienste ***zu*** sicherzustellen;	Kontinuität ihrer Dienste sicherzustellen***, einschließlich einer breiten Konnektivität zwischen Netzen sowie Informationssystemen, -diensten und -Geräten***;

Änderungsantrag 142

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 1 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(1a) CSIRTs müssen mindestens die folgenden technischen Fähigkeiten entwickeln:
	a) Fähigkeit zur Echtzeit-Überwachung oder echtzeitnahen Überwachung von Netzen und Informationssystemen und zur Erkennung von Anomalien;
	b) die Fähigkeit zur Unterstützung der Angriffsabwehr und Angriffserkennung;
	c) die Fähigkeit zur Sammlung und Durchführung komplexer forensischer Datenanalysen und zum Reverse Engineering von Cyber-Bedrohungen;
	d) die Fähigkeit zur Filterung von bösartigem Datenverkehr;
	e) die Fähigkeit zur Durchsetzung strenger Authentifizierungs- und Zugangsberechtigungen und -kontrollen sowie
	f) die Fähigkeit zur Analyse von Cyber-Bedrohungen.

Änderungsantrag 143

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 2 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) Überwachung von Cyberbedrohungen, Schwachstellen und	a) Überwachung von Cyberbedrohungen, Schwachstellen und

Sicherheitsvorfällen auf nationaler Ebene;	Sicherheitsvorfällen auf nationaler Ebene ***und Sammlung von Erkenntnissen über Bedrohungen in Echtzeit;***;

Änderungsantrag 144

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 2 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) Ausgabe von Frühwarnungen und Alarmmeldungen sowie Bekanntmachung und Weitergabe von Informationen über Cyberbedrohungen, Schwachstellen und Sicherheitsvorfälle an die wesentlichen und wichtigen Einrichtungen sowie andere interessierte Kreise;	b) Ausgabe von Frühwarnungen und Alarmmeldungen sowie Bekanntmachung und Weitergabe von Informationen über Cyberbedrohungen, Schwachstellen und Sicherheitsvorfälle an die wesentlichen und wichtigen Einrichtungen sowie andere interessierte Kreise***, möglichst echtzeitnah***;

Änderungsantrag 145

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 2 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) Reaktion auf Sicherheitsvorfälle;	c) Reaktion auf Sicherheitsvorfälle ***und Unterstützung der betroffenen Einrichtungen***;

Änderungsantrag 146

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 2 – Buchstabe e

Vorschlag der Kommission	*Geänderter Text*
e) auf Ersuchen einer Einrichtung Durchführung einer proaktiven Überprüfung der für die Bereitstellung ihrer Dienste verwendeten Netz- und Informationssysteme auf Schwachstellen (Schwachstellenscan);	e) auf Ersuchen einer Einrichtung ***oder im Falle einer ernsthaften Bedrohung für die nationale Sicherheit,*** Durchführung einer proaktiven Überprüfung der für die Bereitstellung ihrer Dienste verwendeten Netz- und Informationssysteme auf Schwachstellen (Schwachstellenscan);

Änderungsantrag 147

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 2 – Buchstabe f a (neu)

Vorschlag der Kommission	*Geänderter Text*
	fa) auf Ersuchen einer Einrichtung die Aktivierung und Konfiguration der Netzwerkprotokollierung zum Schutz von Daten, einschließlich personenbezogener Daten, vor unbefugtem Abgreifen;

Änderungsantrag 148

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 2 – Buchstabe f b (neu)

Vorschlag der Kommission	*Geänderter Text*
	fb) Beitrag zum Einsatz sicherer Instrumente für den Informationsaustausch gemäß Artikel 9 Absatz 3.

Änderungsantrag 149

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 4 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(4) Zur Erleichterung der Zusammenarbeit fördern die CSIRTs die Annahme und Anwendung gemeinsamer oder standardisierter Verfahren für Klassifizierungssysteme und Taxonomien für	(4) Zur Erleichterung der Zusammenarbeit fördern die CSIRTs ***die Automatisierung des Informationsaustauschs,*** die Annahme und Anwendung gemeinsamer oder standardisierter Verfahren für Klassifizierungssysteme und Taxonomien für

Änderungsantrag 150

Vorschlag für eine Richtlinie
Artikel 11 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Mitgliedstaaten stellen sicher, dass Meldungen von Sicherheitsvorfällen**,**	(2) Die Mitgliedstaaten stellen sicher, dass Meldungen von ***erheblichen***

erheblichen Cyberbedrohungen und Beinahe-Vorfällen gemäß ***dieser Richtlinie entweder ihren zuständigen Behörden oder ihren CSIRTs übermittelt werden. Entscheidet ein Mitgliedstaat, dass diese Meldungen nicht an seine CSIRTs zu richten sind, so wird den CSIRTs in dem zur Wahrnehmung ihrer Aufgaben erforderlichen Umfang Zugang zu den Daten*** über ***Sicherheitsvorfälle gewährt, die*** gemäß Artikel 20 ***von wesentlichen oder wichtigen Einrichtungen gemeldet*** werden.

Sicherheitsvorfällen gemäß ***Artikel 20 sowie von Cyberbedrohungen und Beinahe-Vorfällen gemäß Artikel 27*** über ***die zentrale Anlaufstelle*** gemäß Artikel 20 ***Absatz 4a ihren CSIRTs übermittelt*** werden.

Änderungsantrag 151

Vorschlag für eine Richtlinie
Artikel 11 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
(4) Soweit dies zur wirksamen Wahrnehmung der in dieser Richtlinie festgelegten Aufgaben und Pflichten erforderlich ist, sorgen die Mitgliedstaaten für eine angemessene Zusammenarbeit zwischen den zuständigen Behörden ***und*** den zentralen Anlaufstellen ***sowie*** den Strafverfolgungsbehörden, den Datenschutzbehörden, den gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] für kritische Infrastrukturen zuständigen Behörden und den gemäß der Verordnung (EU) XXXX/XXXX des Europäischen Parlaments und des Rates[39] [DORA-Verordnung] in dem jeweiligen Mitgliedstaat benannten nationalen Finanzbehörden.	(4) Soweit dies zur wirksamen Wahrnehmung der in dieser Richtlinie festgelegten Aufgaben und Pflichten erforderlich ist, sorgen die Mitgliedstaaten für eine angemessene Zusammenarbeit zwischen den zuständigen Behörden***,*** den zentralen Anlaufstellen***, den CSIRTs,*** den Strafverfolgungsbehörden, den ***nationalen Regulierungsbehörden oder anderen zuständigen Behörden, die für öffentliche elektronische Kommunikationsnetze oder für öffentlich zugängliche elektronische Kommunikationsdienste gemäß der Richtlinie (EU) 2018/1972 zuständig sind, den*** Datenschutzbehörden, den gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] für kritische Infrastrukturen zuständigen Behörden und den gemäß der Verordnung (EU) XXXX/XXXX des Europäischen Parlaments und des Rates[39] [DORA-Verordnung] in dem jeweiligen Mitgliedstaat benannten nationalen Finanzbehörden***, die im Einklang mit den jeweiligen Zuständigkeiten der Einrichtungen erfolgt***.

[39] [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].

[39] [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].

Änderungsantrag 152

Vorschlag für eine Richtlinie
Artikel 11 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
(5) Die Mitgliedstaaten stellen sicher, dass ihre zuständigen Behörden die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannten zuständigen Behörden regelmäßig über Cybersicherheitsrisiken, Cyberbedrohungen und Sicherheitsvorfälle unterrichten, die als kritische Einrichtungen oder kritischen Einrichtungen gleichgestellte Einrichtungen gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] ermittelte wesentliche Einrichtungen betreffen, sowie über die von den zuständigen Behörden als Reaktion auf diese Risiken und Sicherheitsvorfälle ergriffenen Maßnahmen.	(5) Die Mitgliedstaaten stellen sicher, dass ihre zuständigen Behörden die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannten zuständigen Behörden regelmäßig ***und zeitnah*** über Cybersicherheitsrisiken, Cyberbedrohungen und Sicherheitsvorfälle unterrichten, die als kritische Einrichtungen oder kritischen Einrichtungen gleichgestellte Einrichtungen gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] ermittelte wesentliche Einrichtungen betreffen, sowie über die von den zuständigen Behörden als Reaktion auf diese Risiken und Sicherheitsvorfälle ergriffenen Maßnahmen.

Änderungsantrag 153

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 3 – Unterabsatz 1

Vorschlag der Kommission	*Geänderter Text*
Die Kooperationsgruppe setzt sich aus Vertretern der Mitgliedstaaten, der Kommission und der ENISA zusammen. Der Europäische Auswärtige Dienst nimmt an den Tätigkeiten der Kooperationsgruppe als Beobachter teil. Die Europäischen Aufsichtsbehörden (ESAs) können sich gemäß Artikel 17 Absatz 5 Buchstabe c der Verordnung (EU) XXXX/XXXX [DORA-Verordnung] an den Tätigkeiten der Kooperationsgruppe beteiligen.	Die Kooperationsgruppe setzt sich aus Vertretern der Mitgliedstaaten, der Kommission und der ENISA zusammen. ***Das Europäische Parlament und*** der Europäische Auswärtige Dienst ***nehmen*** an den Tätigkeiten der Kooperationsgruppe als Beobachter teil. Die Europäischen Aufsichtsbehörden (ESAs) können sich gemäß Artikel 17 Absatz 5 Buchstabe c der Verordnung (EU) XXXX/XXXX [DORA-Verordnung] an den Tätigkeiten der

Kooperationsgruppe beteiligen.

Änderungsantrag 154

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 3 – Unterabsatz 2

Vorschlag der Kommission	*Geänderter Text*
Gegebenenfalls kann die Kooperationsgruppe Vertreter der maßgeblichen Interessenträger einladen, an ihren Arbeiten teilzunehmen.	Gegebenenfalls kann die Kooperationsgruppe Vertreter der maßgeblichen Interessenträger ***wie den Europäischen Datenschutzausschuss und Vertreter der Industrie*** einladen, an ihren Arbeiten teilzunehmen.

Änderungsantrag 155

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 4 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) Austausch bewährter Verfahren und Informationsaustausch im Zusammenhang mit der Umsetzung dieser Richtlinie, auch in Bezug auf Cyberbedrohungen, Sicherheitsvorfälle, Schwachstellen, Beinahe-Vorfälle, Sensibilisierungsinitiativen, Schulungen, Übungen und Kompetenzen, Kapazitätsaufbau sowie Normen und technische Spezifikationen;	b) Austausch bewährter Verfahren und Informationsaustausch im Zusammenhang mit der Umsetzung dieser Richtlinie, auch in Bezug auf Cyberbedrohungen, Sicherheitsvorfälle, Schwachstellen, Beinahe-Vorfälle, Sensibilisierungsinitiativen, Schulungen, Übungen und Kompetenzen, Kapazitätsaufbau sowie Normen und technische Spezifikationen ***sowie Bestimmung wesentlicher und wichtiger Einrichtungen***;

Änderungsantrag 156

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 4 – Buchstabe b a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ba) Vornahme einer Bestandsaufnahme der nationalen Lösungen, um die Kompatibilität von Cybersicherheitslösungen zu fördern, die für die einzelnen spezifischen Branchen

	in der gesamten Union angewendet werden;

Änderungsantrag 157

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 4 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) beratender Austausch und Zusammenarbeit mit der Kommission in Bezug auf neue politische Initiativen im Bereich der Cybersicherheit;	c) beratender Austausch und Zusammenarbeit mit der Kommission in Bezug auf neue politische Initiativen im Bereich der Cybersicherheit ***und die allgemeine Kohärenz der sektorspezifischen Anforderungen an die Cybersicherheit***;

Änderungsantrag 158

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 4 – Buchstabe f

Vorschlag der Kommission	*Geänderter Text*
f) Erörterung von Berichten über die in Artikel 16 Absatz 7 genannten Peer Reviews;	f) Erörterung von Berichten über die in Artikel 16 Absatz 7 genannten Peer-Reviews ***und Ausarbeitung von Schlussfolgerungen und Empfehlungen***;

Änderungsantrag 159

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 4 – Buchstabe f a (neu)

Vorschlag der Kommission	*Geänderter Text*
	fa) Durchführung von koordinierten Bewertungen der Sicherheitsrisiken, die gemäß Artikel 19 Absatz 1 eingeleitet werden können, in Zusammenarbeit mit der Kommission und der ENISA;

Änderungsantrag 160

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 4 – Buchstabe k a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ka) Übermittlung von Berichten über die auf strategischer und operativer Ebene gewonnenen Erfahrungen an die Kommission zum Zwecke der Überprüfung gemäß Artikel 35;

Änderungsantrag 161

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 4 – Buchstabe k b (neu)

Vorschlag der Kommission	*Geänderter Text*
	kb) Vorlage einer in Zusammenarbeit mit ENISA, Europol und nationalen Strafverfolgungsbehörden erarbeiteten jährlichen Bewertung der Drittländer, in denen Ransomware-Kriminelle ihr Unwesen treiben können.

Änderungsantrag 162

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 8

Vorschlag der Kommission	*Geänderter Text*
(8) Die Kooperationsgruppe tagt regelmäßig, mindestens aber ***einmal*** jährlich gemeinsam mit der mit der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] eingerichteten Gruppe für die Resilienz kritischer Einrichtungen, um die strategische Zusammenarbeit und den Informationsaustausch zu ***fördern***.	(8) Die Kooperationsgruppe tagt regelmäßig, mindestens aber ***zweimal*** jährlich gemeinsam mit der mit der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] eingerichteten Gruppe für die Resilienz kritischer Einrichtungen, um die strategische Zusammenarbeit und den Informationsaustausch zu ***erleichtern***.

Änderungsantrag 163

Vorschlag für eine Richtlinie
Artikel 13 – Absatz 3 – Buchstabe a 4 (neu)

Vorschlag der Kommission	*Geänderter Text*
	aa) Erleichterung des Transfers und

	des Austauschs von Technologie sowie relevanten Maßnahmen, Strategien, bewährten Verfahren und Rahmenbedingungen zwischen den CSIRTs;

Änderungsantrag 164

Vorschlag für eine Richtlinie
Artikel 13 – Absatz 3 – Buchstabe b a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ba) Gewährleistung der Interoperabilität in Bezug auf die Standards des Informationsaustauschs;

Änderungsantrag 165

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Zur Unterstützung des koordinierten Managements massiver Cybersicherheitsvorfälle und -krisen auf operativer Ebene und zur Gewährleistung eines regelmäßigen ***Informationsaustauschs*** zwischen den Mitgliedstaaten und den Organen, Einrichtungen und Agenturen der Union wird hiermit das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (European Cyber Crises Liaison Organisation Network, EU-CyCLONe) eingerichtet.	(1) Zur Unterstützung des koordinierten Managements massiver Cybersicherheitsvorfälle und -krisen auf operativer Ebene und zur Gewährleistung eines regelmäßigen ***Austauschs relevanter Informationen*** zwischen den Mitgliedstaaten und den Organen, Einrichtungen und Agenturen der Union wird hiermit das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (European Cyber Crises Liaison Organisation Network, EU-CyCLONe) eingerichtet.

Änderungsantrag 166

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) EU-CyCLONe setzt sich aus den Vertretern der gemäß Artikel 7 benannten für das Krisenmanagement zuständigen	(2) EU-CyCLONe setzt sich aus den Vertretern der gemäß Artikel 7 benannten für das Krisenmanagement zuständigen

Behörden der Mitgliedstaaten, der Kommission und der ENISA zusammen. ENISA führt die Sekretariatsgeschäfte des ***Netzwerks*** und unterstützt den sicheren Informationsaustausch.	Behörden der Mitgliedstaaten, der Kommission und der ENISA zusammen. ENISA führt die Sekretariatsgeschäfte des ***EU-CyCLONe*** und unterstützt den sicheren Informationsaustausch.

Änderungsantrag 167

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
(5) EU-CyCLONe erstattet der Kooperationsgruppe regelmäßig Bericht über ***Cyberbedrohungen,*** Sicherheitsvorfälle und Trends, wobei der Schwerpunkt insbesondere auf deren Auswirkungen auf wesentliche und wichtige Einrichtungen liegt.	(5) EU-CyCLONe erstattet der Kooperationsgruppe regelmäßig Bericht über Sicherheitsvorfälle ***großen Ausmaßes*** und ***Krisen sowie*** Trends, wobei der Schwerpunkt insbesondere auf deren Auswirkungen auf wesentliche und wichtige Einrichtungen liegt.

Änderungsantrag 168

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 1 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(1) Die ENISA veröffentlicht in Zusammenarbeit mit der Kommission einen zweijährlichen Bericht über den Stand der Cybersicherheit in der Union. Dieser Bericht muss insbesondere Folgendes enthalten:	(1) Die ENISA veröffentlicht in Zusammenarbeit mit der Kommission einen zweijährlichen Bericht über den Stand der Cybersicherheit in der Union ***und legt ihn dem Europäischen Parlament vor***. Dieser Bericht muss ***in einem maschinenlesbaren Format erstellt werden und*** insbesondere Folgendes enthalten:

Änderungsantrag 169

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 1 – Buchstabe a a (neu)

Vorschlag der Kommission	*Geänderter Text*
	aa) den allgemeinen Grad von Cybersicherheitsbewusstsein und -hygiene bei den Bürgerinnen und Bürgern sowie

des allgemeinen Sicherheitsniveaus bei vernetzten Geräten;

Änderungsantrag 170

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 1 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) einen Cybersicherheitsindex für eine aggregierte Bewertung des Entwicklungsstands der Cybersicherheitskapazitäten**.**	c) einen Cybersicherheitsindex für eine aggregierte Bewertung des Entwicklungsstands der Cybersicherheitskapazitäten ***in der gesamten Union, einschließlich der Angleichung der nationalen Cybersicherheitsstrategien der Mitgliedstaaten;***

Änderungsantrag 171

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Der Bericht muss insbesondere politische Empfehlungen zur Erhöhung des Cybersicherheitsniveaus in der gesamten Union und eine Zusammenfassung der Ergebnisse der von der ENISA gemäß Artikel 7 Absatz 6 der Verordnung (EU) 2019/881 für den entsprechenden Zeitraum erstellten technischen EU-Cybersicherheitslageberichte umfassen.	(2) Der Bericht muss insbesondere ***die Ermittlung von Hindernissen und*** politische Empfehlungen zur Erhöhung des Cybersicherheitsniveaus in der gesamten Union und eine Zusammenfassung der Ergebnisse der von der ENISA gemäß Artikel 7 Absatz 6 der Verordnung (EU) 2019/881 für den entsprechenden Zeitraum erstellten technischen EU-Cybersicherheitslageberichte umfassen.

Änderungsantrag 172

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 2 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(2a) Die ENISA erarbeitet in Zusammenarbeit mit der Kommission und unter Anleitung der Kooperationsgruppe und des CSIRT-Netzes die Methodik,

	einschließlich der einschlägigen Variablen des in Absatz 1 Buchstabe c genannten Cybersicherheitsindexes.

Änderungsantrag 173

Vorschlag für eine Richtlinie
Artikel 16 – Absatz 1 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(1) Nach Konsultation der Kooperationsgruppe und der ENISA legt die Kommission spätestens 18 Monate nach Inkrafttreten dieser Richtlinie die Methode und den Inhalt eines Peer-Review-Systems zur Bewertung der Wirksamkeit der Cybersicherheitskonzepte der Mitgliedstaaten fest. Die Peer Reviews werden von technischen Sachverständigen für Cybersicherheit aus anderen als den überprüften Mitgliedstaaten durchgeführt und erstrecken sich mindestens auf Folgendes:	(1) Nach Konsultation der Kooperationsgruppe und der ENISA legt die Kommission spätestens zum **...** ***[***18 Monate nach Inkrafttreten dieser Richtlinie***]*** die Methode und den Inhalt eines Peer-Review-Systems zur Bewertung der Wirksamkeit der Cybersicherheitskonzepte der Mitgliedstaaten fest. Die Peer-Reviews werden ***in Absprache mit der ENISA*** von technischen Sachverständigen für Cybersicherheit aus ***wenigstens zwei*** anderen als den überprüften Mitgliedstaaten durchgeführt und erstrecken sich mindestens auf Folgendes:

Änderungsantrag 174

Vorschlag für eine Richtlinie
Artikel 16 – Absatz 1 – Ziffer iii

Vorschlag der Kommission	*Geänderter Text*
iii) die operativen Kapazitäten und die Wirksamkeit der CSIRTs;	iii) die operativen Kapazitäten und die Wirksamkeit der CSIRTs ***bei der Wahrnehmung ihrer Aufgaben***;

Änderungsantrag 175

Vorschlag für eine Richtlinie
Artikel 16 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Die organisatorischen Aspekte der Peer Reviews werden von der Kommission	(3) Die organisatorischen Aspekte der Peer Reviews werden von der Kommission

mit Unterstützung der ENISA beschlossen und beruhen nach Konsultation der Kooperationsgruppe auf Kriterien, die in der in Absatz 1 genannten Methode festgelegt sind. Bei den Peer Reviews werden für alle Mitgliedstaaten und Sektoren die in Absatz 1 genannten Aspekte bewertet, einschließlich gezielter Fragen, die speziell einen oder mehrere Mitgliedstaaten oder einen oder mehrere Sektoren betreffen.	mit Unterstützung der ENISA beschlossen und beruhen nach Konsultation der Kooperationsgruppe auf Kriterien, die in der in Absatz 1 genannten Methode festgelegt sind. Bei den Peer Reviews werden für alle Mitgliedstaaten und Sektoren die in Absatz 1 genannten Aspekte bewertet, einschließlich gezielter Fragen, die speziell einen oder mehrere Mitgliedstaaten oder einen oder mehrere Sektoren betreffen. ***Die benannten Sachverständigen, die die Überprüfung durchführen, teilen dem Mitgliedstaat, der der Peer-Review unterliegt, diese gezielten Fragen vor Beginn der Überprüfung mit.***

Änderungsantrag 176

Vorschlag für eine Richtlinie
Artikel 16 – Absatz 3 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(3a) Vor Beginn des Peer-Review-Verfahrens führt der Mitgliedstaat, der der Peer-Review unterliegt, eine Selbstbewertung der überprüften Aspekte durch und legt diese Selbstbewertung den benannten Sachverständigen vor.

Änderungsantrag 177

Vorschlag für eine Richtlinie
Artikel 16 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
(4) Die Peer Reviews müssen tatsächliche oder virtuelle Besuche am Standort und Möglichkeiten zum Austausch außerhalb des Standorts umfassen. In Anbetracht des Grundsatzes der guten Zusammenarbeit stellen die überprüften Mitgliedstaaten den benannten Sachverständigen die für die Bewertung der überprüften Aspekte erforderlichen Informationen zur Verfügung. Sämtliche	(4) Die Peer Reviews müssen tatsächliche oder virtuelle Besuche am Standort und Möglichkeiten zum Austausch außerhalb des Standorts umfassen. In Anbetracht des Grundsatzes der guten Zusammenarbeit stellen die überprüften Mitgliedstaaten den benannten Sachverständigen die für die Bewertung der überprüften Aspekte erforderlichen Informationen zur Verfügung. ***Die***

durch das Peer-Review-Verfahren erlangten Informationen dürfen nur zu diesem Zweck verwendet werden. Die an der Peer Review beteiligten Sachverständigen geben keine sensiblen oder vertraulichen Informationen, die im Laufe der Peer Review erlangt wurden, an Dritte weiter.

Kommission entwickelt in Zusammenarbeit mit der ENISA geeignete Verhaltenskodizes zur Untermauerung der Arbeitsmethoden der benannten Sachverständigen. Sämtliche durch das Peer-Review-Verfahren erlangten Informationen dürfen nur zu diesem Zweck verwendet werden. Die an der Peer Review beteiligten Sachverständigen geben keine sensiblen oder vertraulichen Informationen, die im Laufe der Peer Review erlangt wurden, an Dritte weiter.

Änderungsantrag 178

Vorschlag für eine Richtlinie
Artikel 16 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
(6) Die Mitgliedstaaten stellen sicher, dass jegliches Risiko eines Interessenkonflikts im Zusammenhang mit den benannten Sachverständigen den anderen Mitgliedstaaten, der Kommission und der ENISA ***unverzüglich*** offengelegt wird.	(6) Die Mitgliedstaaten stellen sicher, dass jegliches Risiko eines Interessenkonflikts im Zusammenhang mit den benannten Sachverständigen den anderen Mitgliedstaaten, der Kommission und der ENISA ***vor Beginn des Peer-Review-Verfahrens*** offengelegt wird.

Änderungsantrag 179

Vorschlag für eine Richtlinie
Artikel 16 – Absatz 7

Vorschlag der Kommission	*Geänderter Text*
(7) Die an Peer Reviews beteiligten Sachverständigen erstellen Berichte über die Ergebnisse und Schlussfolgerungen der Peer Reviews. Die Berichte werden der Kommission, der Kooperationsgruppe, dem CSIRT-Netzwerk und der ENISA vorgelegt. Sie werden in der Kooperationsgruppe und im CSIRT-Netzwerk erörtert. Die Berichte können auf der speziellen Website der Kooperationsgruppe veröffentlicht werden.	(7) Die an Peer Reviews beteiligten Sachverständigen erstellen Berichte über die Ergebnisse und Schlussfolgerungen der Peer Reviews. ***Die Berichte enthalten Empfehlungen zur Verbesserung der im Peer-Review-Verfahren behandelten Aspekte.*** Die Berichte werden der Kommission, der Kooperationsgruppe, dem CSIRT-Netzwerk und der ENISA vorgelegt. Sie werden in der Kooperationsgruppe und im CSIRT-Netzwerk erörtert. Die Berichte können auf

der speziellen Website der Kooperationsgruppe veröffentlicht werden. ***Dies gilt nicht für sensible oder vertrauliche Informationen.***

Änderungsantrag 180

Vorschlag für eine Richtlinie
Artikel 17 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Mitgliedstaaten stellen sicher, dass die Mitglieder der Leitungsorgane regelmäßig an spezifischen Schulungen teilnehmen, ***um*** ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf ***den Betrieb*** der Einrichtung ***zu*** erwerben.	(2) Die Mitgliedstaaten stellen sicher, dass die Mitglieder der Leitungsorgane ***wesentlicher und wichtiger Einrichtungen*** regelmäßig an spezifischen Schulungen teilnehmen, ***und fordern wesentliche und wichtige Einrichtungen auf, allen Mitarbeitern regelmäßig entsprechende Schulungen anzubieten, damit sie*** ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf ***die von*** der Einrichtung ***erbrachten Dienstleistungen*** erwerben ***können***.

Änderungsantrag 181

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen ***bei der*** Erbringung ihrer Dienste nutzen, zu beherrschen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das	(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische***, operative*** und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen ***für ihren Betrieb und für die*** Erbringung ihrer Dienste nutzen, zu beherrschen ***und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu***

dem bestehenden Risiko angemessen ist.	***halten***. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ***sowie europäischer oder internationaler Normen*** ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist.

Änderungsantrag 182

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 2 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) Bewältigung von Sicherheitsvorfällen ***(Prävention und Erkennung von Sicherheitsvorfällen und Reaktion auf Sicherheitsvorfälle)***;	b) Bewältigung von Sicherheitsvorfällen;

Änderungsantrag 183

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 2 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) Aufrechterhaltung des Betriebs und Krisenmanagement;	c) Aufrechterhaltung des Betriebs***, wie Backup-Management*** und ***Wiederherstellung nach einem Notfall, sowie*** Krisenmanagement;

Änderungsantrag 184

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 2 – Buchstabe d

Vorschlag der Kommission	*Geänderter Text*
d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren Anbietern oder Diensteanbietern ***beispielsweise Anbietern von Datenspeicher- und Datenverarbeitungsdiensten oder verwalteten Sicherheitsdiensten (MSS)***;	d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren Anbietern oder Diensteanbietern;

Änderungsantrag 185

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 2 – Buchstabe f

Vorschlag der Kommission	*Geänderter Text*
f) Konzepte und Verfahren (Erprobung und Prüfung) zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;	f) Konzepte und Verfahren (***Schulungen,*** Erprobung und Prüfung) zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;

Änderungsantrag 186

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 2 – Buchstabe f a (neu)

Vorschlag der Kommission	*Geänderter Text*
	fa) grundlegende Computerhygienepraktiken und Schulungen im Bereich Cybersicherheit;

Änderungsantrag 187

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 2 – Buchstabe g

Vorschlag der Kommission	*Geänderter Text*
g) Einsatz von Kryptografie ***und*** Verschlüsselung***.***	g) ***gegebenenfalls*** Einsatz von Kryptografie***, wie*** Verschlüsselung***;***

Änderungsantrag 188

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 2 – Buchstabe g a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ga) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Änderungsantrag 189
Vorschlag für eine Richtlinie
Artikel 18 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
(4) Die Mitgliedstaaten stellen sicher, dass Einrichtungen, die feststellen, dass ihre Dienste oder Aufgaben die Anforderungen nach Absatz 2 nicht erfüllen, unverzüglich alle erforderlichen Korrekturmaßnahmen ergreifen, um den betreffenden Dienst mit den Anforderungen in Einklang zu bringen.	(4) Die Mitgliedstaaten stellen sicher, dass Einrichtungen, die feststellen, dass ihre Dienste oder Aufgaben die Anforderungen nach Absatz 2 nicht erfüllen, unverzüglich alle erforderlichen***, angemessenen und verhältnismäßigen*** Korrekturmaßnahmen ergreifen, um den betreffenden Dienst mit den Anforderungen in Einklang zu bringen.

Änderungsantrag 190

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
(5) Die Kommission kann Durchführungsrechtsakte erlassen, um die technischen und methodischen Spezifikationen für die in Absatz 2 genannten Elemente festzulegen. Bei der Ausarbeitung dieser Rechtsakte verfährt die Kommission nach dem Prüfverfahren gemäß Artikel 37 Absatz 2 und beachtet dabei so weit wie möglich internationale und europäische Normen sowie die einschlägigen technischen Spezifikationen.	***entfällt***

Änderungsantrag 191

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
(6) Der Kommission wird die Befugnis übertragen, zur Ergänzung der in Absatz 2 genannten Elemente delegierte Rechtsakte gemäß Artikel 36 zu erlassen, um neuen Cyberbedrohungen, technologischen	(6) Der Kommission wird die Befugnis übertragen, zur Ergänzung der in Absatz 2 genannten Elemente delegierte Rechtsakte gemäß Artikel 36 zu erlassen, um neuen Cyberbedrohungen, technologischen

Entwicklungen oder sektorspezifischen Besonderheiten Rechnung zu tragen.	Entwicklungen oder sektorspezifischen Besonderheiten Rechnung zu tragen***, und um diese Richtlinie durch die Festlegung der technischen und methodischen Spezifikationen der Maßnahmen nach Absatz 2 dieses Artikels zu ergänzen***.

Änderungsantrag 192

Vorschlag für eine Richtlinie
Artikel 19 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Die Kooperationsgruppe kann in Zusammenarbeit mit der Kommission und der ENISA koordinierte Risikobewertungen in Bezug auf die Sicherheit der Lieferketten bestimmter kritischer ***IKT-Dienste***, ***-Systeme*** oder ***-Produkte*** unter Berücksichtigung technischer und erforderlichenfalls nichttechnischer Risikofaktoren durchführen.	(1) Die Kooperationsgruppe kann in Zusammenarbeit mit der Kommission und der ENISA koordinierte Risikobewertungen in Bezug auf die Sicherheit der Lieferketten bestimmter kritischer ***Dienste***, ***Systeme*** oder ***Produkte im Bereich der IKT und IKS (Informations- und Kommunikationssysteme)*** unter Berücksichtigung technischer und erforderlichenfalls nichttechnischer Risikofaktoren durchführen.

Änderungsantrag 193

Vorschlag für eine Richtlinie
Artikel 19 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Kommission legt nach Konsultation der Kooperationsgruppe und der ENISA fest, welche spezifischen kritischen ***IKT-Dienste***, -Systeme oder -Produkte der koordinierten Risikobewertung nach Absatz 1 unterzogen werden können***.***	(2) Die Kommission legt nach Konsultation der Kooperationsgruppe und der ENISA ***sowie gegebenenfalls einschlägiger Interessenträger*** fest, welche spezifischen kritischen ***IKT- und IKS-Dienste***, -Systeme oder -Produkte der koordinierten Risikobewertung nach Absatz 1 unterzogen werden können

Änderungsantrag 194

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen ***den zuständigen Behörden oder*** dem CSIRT gemäß den Absätzen 3 und 4 unverzüglich jeden Sicherheitsvorfall melden***, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste hat. Gegebenenfalls unterrichten diese Einrichtungen die Empfänger ihrer Dienste unverzüglich über Sicherheitsvorfälle, die die Erbringung des jeweiligen Dienstes beeinträchtigen könnten***. Die Mitgliedstaaten stellen sicher, dass diese Einrichtungen unter anderem alle Informationen übermitteln, die es ***den zuständigen Behörden oder*** dem CSIRT ermöglichen zu ermitteln, ob der Sicherheitsvorfall grenzübergreifende Auswirkungen hat.	(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen dem CSIRT gemäß den Absätzen 3 und 4 unverzüglich jeden ***erheblichen*** Sicherheitsvorfall melden. Die Mitgliedstaaten stellen sicher, dass diese Einrichtungen unter anderem alle Informationen übermitteln, die es dem CSIRT ermöglichen zu ermitteln, ob der Sicherheitsvorfall grenzübergreifende Auswirkungen hat.

Änderungsantrag 195

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen den zuständigen Behörden oder dem CSIRT unverzüglich jede von diesen Einrichtungen ermittelte erhebliche Cyberbedrohung melden, die nach deren Auffassung möglicherweise zu einem erheblichen Sicherheitsvorfall hätte führen können.	
Gegebenenfalls unterrichten diese Einrichtungen die potenziell von einer erheblichen Cyberbedrohung betroffenen Empfänger ihrer Dienste unverzüglich über alle Maßnahmen oder Abhilfemaßnahmen, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. Die Einrichtungen informieren diese Empfänger	Gegebenenfalls ***stellen die Mitgliedstaaten sicher, dass wesentliche und wichtige Einrichtungen die*** Empfänger ihrer Dienste unverzüglich über ***Schutzmaßnahmen*** oder Abhilfemaßnahmen ***bei bestimmten Sicherheitsvorfällen und bekannten Risiken informieren, die von den Empfängern ergriffen werden*** können.

gegebenenfalls auch über die Bedrohung selbst. Mit der Meldung wird keine höhere Haftung der meldenden Einrichtung begründet.	Die Einrichtungen informieren ***die*** Empfänger ***ihrer Dienste*** gegebenenfalls über ***den Sicherheitsvorfall oder das bekannte Risiko*** selbst. ***Die Unterrichtung der Dienstleistungsempfänger erfolgt auf*** der ***Grundlage bestmöglichen Bemühens und führt nicht zu einer höheren*** Haftung der meldenden Einrichtung.

Änderungsantrag 196

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 3 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(3) Ein Sicherheitsvorfall ***gilt als*** erheblich, ***wenn***	(3) ***Um zu bestimmen, ob*** ein Sicherheitsvorfall erheblich ***ist***, ***werden, sofern verfügbar, die folgenden Parameter berücksichtigt:***

Änderungsantrag 197

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 3 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) ***der*** Sicherheitsvorfall ***erhebliche Betriebsstörungen oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder potenziell verursachen könnte***;	a) ***die Zahl der von dem*** Sicherheitsvorfall ***betroffenen Empfänger der Dienstleistungen;***

Änderungsantrag 198

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 3 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) ***der Sicherheitsvorfall andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Verluste geschädigt hat oder potenziell schädigen könnte.***	b) ***die Dauer des Sicherheitsvorfalls;***

Änderungsantrag 199

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 3 – Buchstabe b a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ba) die geografische Ausdehnung des von dem Sicherheitsvorfall betroffenen Gebiets;

Änderungsantrag 200

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 3 – Buchstabe b b (neu)

Vorschlag der Kommission	*Geänderter Text*
	bb) das Ausmaß, in dem die Funktion und Kontinuität des Dienstes durch den Sicherheitsvorfall beeinträchtigt wird;

Änderungsantrag 201

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 3 – Buchstabe b c (neu)

Vorschlag der Kommission	*Geänderter Text*
	bc) das Ausmaß der Auswirkungen des Sicherheitsvorfalls auf wirtschaftliche und gesellschaftliche Tätigkeiten.

Änderungsantrag 202

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Unterabsatz 1 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
Die Mitgliedstaaten stellen sicher, dass die betreffenden Einrichtungen ***den zuständigen Behörden oder*** dem CSIRT für die Zwecke der Meldung nach Absatz 1 Folgendes übermitteln:	Die Mitgliedstaaten stellen sicher, dass die betreffenden Einrichtungen dem CSIRT für die Zwecke der Meldung nach Absatz 1 Folgendes übermitteln:

Änderungsantrag 203

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Unterabsatz 1 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) ***unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des Sicherheitsvorfalls***, eine erste Meldung, ***in*** der ***gegebenenfalls angegeben wird, ob*** der ***Sicherheitsvorfall vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist;***	a) eine erste Meldung ***des erheblichen Sicherheitsvorfalls***, ***die Informationen enthält***, ***die*** der ***meldenden Einrichtung auf*** der ***Grundlage bestmöglichen Bemühens zur Verfügung stehen, und zwar wie folgt:***

Änderungsantrag 204

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Unterabsatz 1 – Buchstabe a – Ziffer i (neu)

Vorschlag der Kommission	*Geänderter Text*
	i) Bei Sicherheitsvorfällen, die die Verfügbarkeit der von der Einrichtung erbrachten Dienste erheblich beeinträchtigen, ist das CSIRT unverzüglich, auf jeden Fall aber innerhalb von 24 Stunden nach Bekanntwerden des Sicherheitsvorfalls zu benachrichtigen.

Änderungsantrag 205

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Unterabsatz 1 – Buchstabe a – Ziffer ii (neu)

Vorschlag der Kommission	*Geänderter Text*
	ii) Bei Sicherheitsvorfällen, die erhebliche Auswirkungen auf die Einrichtung haben und nicht nur die Verfügbarkeit der von dieser Einrichtung erbrachten Dienste betreffen, ist das CSIRT unverzüglich, auf jeden Fall aber innerhalb von 72 Stunden nach Bekanntwerden des Sicherheitsvorfalls zu benachrichtigen.

Änderungsantrag 206

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Unterabsatz 1 – Buchstabe a – Ziffer iii (neu)

Vorschlag der Kommission	*Geänderter Text*
	iii) Bei Sicherheitsvorfällen, die erhebliche Auswirkungen auf die Dienste eines Vertrauensdiensteanbieters im Sinne von Artikel 3 Nummer 19 der Verordnung (EU) Nr. 910/2014 oder auf die von diesem Vertrauensdiensteanbieter vorgehaltenen personenbezogenen Daten haben, ist das CSIRT unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Bekanntwerden des Sicherheitsvorfalls zu benachrichtigen.

Änderungsantrag 207

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Unterabsatz 1 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) ***auf Ersuchen einer zuständigen Behörde oder eines CSIRT*** einen Zwischenbericht über relevante Statusaktualisierungen;	b) einen Zwischenbericht über relevante Statusaktualisierungen ***auf Ersuchen eines CSIRT***;

Änderungsantrag 208

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Unterabsatz 1 – Buchstabe c – Einleitung

Vorschlag der Kommission	*Geänderter Text*
c) spätestens einen Monat nach Vorlage ***des Berichts gemäß Buchstabe a*** einen ***Abschlussbericht***, der mindestens Folgendes enthält:	c) spätestens einen Monat nach Vorlage ***der ersten Meldung*** einen ***umfassenden Bericht***, der mindestens Folgendes enthält:

Änderungsantrag 209

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Unterabsatz 1 – Buchstabe c a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ca) Im Fall eines Sicherheitsvorfalls, der bei Vorlage des umfassenden Berichts gemäß Buchstabe c noch aussteht, ist einen Monat nach der Bewältigung des Sicherheitsvorfalls ein Abschlussbericht vorzulegen.

Änderungsantrag 210

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Unterabsatz 2

Vorschlag der Kommission	*Geänderter Text*
Die Mitgliedstaaten sehen vor, dass die betreffende Einrichtung in hinreichend begründeten Fällen und im Einvernehmen mit ***den zuständigen Behörden oder*** dem CSIRT von den unter ***den Buchstaben*** a und c festgelegten Fristen abweichen kann.	Die Mitgliedstaaten sehen vor, dass die betreffende Einrichtung in hinreichend begründeten Fällen und im Einvernehmen mit dem CSIRT von den unter ***Buchstabe*** a ***Ziffern i*** und ***ii sowie Buchstabe*** c festgelegten Fristen abweichen kann. ***Die Mitgliedstaaten stellen die Vertraulichkeit und den angemessenen Schutz sensibler Informationen über Sicherheitsvorfälle, die an die CSIRTs weitergegeben werden, sicher und erlassen Maßnahmen und Verfahren für die gemeinsame Nutzung und Wiederverwendung von Informationen über Sicherheitsvorfälle.***

Änderungsantrag 211

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(4a) Die Mitgliedstaaten richten eine zentrale Anlaufstelle für alle Meldungen ein, die aufgrund dieser Richtlinie sowie anderer EU-Rechtsvorschriften vorgeschrieben sind. Die ENISA hat in Zusammenarbeit mit der Kooperationsgruppe mittels Leitlinien einheitliche Meldemuster zu erstellen und kontinuierlich zu verbessern, die die

Erteilung der im Unionsrecht geforderten Informationen vereinfachen und straffen und den Aufwand für meldende Einrichtungen verringern.

Änderungsantrag 212

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	(4b) Wesentliche und wichtige Einrichtungen nach Artikel 24 Absatz 1 können die Anforderungen von Absatz 1 des vorliegenden Artikels erfüllen, indem sie das CSIRT des Mitgliedstaats, in dem sie ihre Hauptniederlassung in der Union haben, sowie die wesentlichen und wichtigen Einrichtungen, für die sie Dienstleistungen erbringen, über jeden erheblichen Sicherheitsvorfall, von dem bekannt ist, dass er Auswirkungen auf den Dienstleistungsempfänger hat, unterrichten.

Änderungsantrag 213

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
(5) ***Die zuständigen nationalen Behörden oder*** das CSIRT übermitteln der meldenden Einrichtung innerhalb von 24 Stunden nach Eingang der ersten Meldung gemäß Absatz 4 Buchstabe a eine Antwort, einschließlich einer ersten Rückmeldung zu dem Sicherheitsvorfall und, auf Ersuchen der Einrichtung, Orientierungshilfen für die Durchführung möglicher Abhilfemaßnahmen. ***Wurde die in Absatz 1 genannte Meldung nicht dem CSIRT übermittelt, werden die Orientierungshilfen von der zuständigen Behörde in Zusammenarbeit mit dem CSIRT bereitgestellt.*** Das CSIRT leistet	(5) Das CSIRT übermitteln der meldenden Einrichtung innerhalb von 24 Stunden nach Eingang der ersten Meldung gemäß Absatz 4 Buchstabe a eine Antwort, einschließlich einer ersten Rückmeldung zu dem Sicherheitsvorfall und, auf Ersuchen der Einrichtung, Orientierungshilfen ***und umsetzbare Ratschläge*** für die Durchführung möglicher Abhilfemaßnahmen. Das CSIRT leistet auf Ersuchen der betreffenden Einrichtung zusätzliche technische Unterstützung. Wird bei dem Sicherheitsvorfall ein krimineller Hintergrund vermutet, ***gibt*** das CSIRT

auf Ersuchen der betreffenden Einrichtung zusätzliche technische Unterstützung. Wird bei dem Sicherheitsvorfall ein krimineller Hintergrund vermutet, ***geben die zuständigen nationalen Behörden oder*** das CSIRT ferner Orientierungshilfen für die Meldung des Sicherheitsvorfalls an die Strafverfolgungsbehörden.

ferner Orientierungshilfen für die Meldung des Sicherheitsvorfalls an die Strafverfolgungsbehörden. ***Das CSIRT kann Informationen über den Sicherheitsvorfall an andere wichtige und wesentliche Einrichtungen weitergeben, wobei die Vertraulichkeit der von der meldenden Einrichtung bereitgestellten Informationen sichergestellt wird.***

Änderungsantrag 214

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
(6) Gegebenenfalls und insbesondere, wenn der in Absatz 1 genannte Sicherheitsvorfall zwei oder mehr Mitgliedstaaten betrifft, unterrichtet ***die zuständige Behörde oder*** das CSIRT, ***der bzw.*** dem die Meldung erstattet wurde, die anderen betroffenen Mitgliedstaaten und die ENISA über den Sicherheitsvorfall. Dabei wahren die zuständigen Behörden, die CSIRTs und die zentralen Anlaufstellen im Einklang mit dem Unionsrecht oder mit den dem Unionsrecht entsprechenden nationalen Rechtsvorschriften die Sicherheit und das wirtschaftliche Interesse der Einrichtung sowie die Vertraulichkeit der bereitgestellten Informationen.	(6) Gegebenenfalls und insbesondere, wenn der in Absatz 1 genannte Sicherheitsvorfall zwei oder mehr Mitgliedstaaten betrifft, unterrichtet das CSIRT, dem die Meldung erstattet wurde, die anderen betroffenen Mitgliedstaaten und die ENISA über den Sicherheitsvorfall ***und liefert relevante Informationen***. Dabei wahren die zuständigen Behörden, die CSIRTs und die zentralen Anlaufstellen im Einklang mit dem Unionsrecht oder mit den dem Unionsrecht entsprechenden nationalen Rechtsvorschriften die Sicherheit und das wirtschaftliche Interesse der Einrichtung sowie die Vertraulichkeit der bereitgestellten Informationen.

Änderungsantrag 215

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 7

Vorschlag der Kommission	*Geänderter Text*
(7) Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen Sicherheitsvorfall zu verhindern oder einen laufenden Sicherheitsvorfall zu bewältigen oder liegt die Offenlegung des Sicherheitsvorfalls anderweitig im öffentlichen Interesse, so können ***die***	(7) Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen Sicherheitsvorfall zu verhindern oder einen laufenden Sicherheitsvorfall zu bewältigen oder liegt die Offenlegung des Sicherheitsvorfalls anderweitig im öffentlichen Interesse, so können das

zuständige Behörde oder das CSIRT sowie gegebenenfalls ***die Behörden oder*** die CSIRTs anderer betroffener Mitgliedstaaten nach Konsultation der betroffenen Einrichtung die Öffentlichkeit über den Sicherheitsvorfall informieren oder die Einrichtung auffordern, dies zu tun.

CSIRT sowie gegebenenfalls die CSIRTs anderer betroffener Mitgliedstaaten nach Konsultation der betroffenen Einrichtung die Öffentlichkeit über den Sicherheitsvorfall informieren oder die Einrichtung auffordern, dies zu tun.

Änderungsantrag 216

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 7 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(7a) Die CSIRTs übermitteln der zentralen Anlaufstelle und gegebenenfalls den zuständigen Behörden unverzüglich die Informationen über die gemäß Absatz 1 gemeldeten erheblichen Sicherheitsvorfälle.

Änderungsantrag 217

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 8

Vorschlag der Kommission	*Geänderter Text*
(8) Auf Ersuchen ***der zuständigen Behörde oder*** des CSIRT leitet die zentrale Anlaufstelle die nach den ***Absätzen*** 1 ***und 2*** eingegangenen Meldungen an die zentralen Anlaufstellen der anderen betroffenen Mitgliedstaaten weiter.	(8) Auf Ersuchen des CSIRT leitet die zentrale Anlaufstelle die nach den ***Absatz*** 1 eingegangenen Meldungen an die zentralen Anlaufstellen der anderen betroffenen Mitgliedstaaten weiter***, wobei sie die Vertraulichkeit und den angemessenen Schutz der von der meldenden Einrichtung übermittelten Informationen sicherstellt***.

Änderungsantrag 218

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 9

Vorschlag der Kommission	*Geänderter Text*
(9) Die zentrale Anlaufstelle legt der	(9) Die zentrale Anlaufstelle legt der

ENISA monatlich einen zusammenfassenden Bericht vor, der anonymisierte und aggregierte Daten zu Sicherheitsvorfällen, erheblichen Cyberbedrohungen und Beinahe-Vorfällen enthält, die gemäß ***den Absätzen*** 1 ***und 2 und gemäß*** Artikel 27 gemeldet wurden. Um zur Bereitstellung vergleichbarer Informationen beizutragen, kann die ENISA technische Leitlinien zu den Parametern der in den zusammenfassenden Bericht aufzunehmenden Angaben herausgeben.

ENISA monatlich einen zusammenfassenden Bericht vor, der anonymisierte und aggregierte Daten zu Sicherheitsvorfällen, erheblichen Cyberbedrohungen und Beinahe-Vorfällen enthält, die gemäß ***Absatz*** 1 ***des vorliegenden Artikels und*** Artikel 27 gemeldet wurden. Um zur Bereitstellung vergleichbarer Informationen beizutragen, kann die ENISA technische Leitlinien zu den Parametern der in den zusammenfassenden Bericht aufzunehmenden Angaben herausgeben.

Änderungsantrag 219

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 10

Vorschlag der Kommission	*Geänderter Text*
(10) Die zuständigen Behörden stellen den gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannten zuständigen Behörden Informationen über Sicherheitsvorfälle und Cyberbedrohungen zur Verfügung, die nach ***den Absätzen*** 1 und ***2*** von wesentlichen Einrichtungen, die im Sinne der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] als kritische Einrichtungen oder als kritischen Einrichtungen gleichwertige Einrichtungen gelten, gemeldet wurden.	(10) Die zuständigen Behörden stellen den gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannten zuständigen Behörden Informationen über Sicherheitsvorfälle und Cyberbedrohungen zur Verfügung, die nach ***Absatz*** 1 ***des vorliegenden Artikels*** und Artikel ***27*** von wesentlichen Einrichtungen, die im Sinne der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] als kritische Einrichtungen oder als kritischen Einrichtungen gleichwertige Einrichtungen gelten, gemeldet wurden.

Änderungsantrag 220

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 11

Vorschlag der Kommission	*Geänderter Text*
(11) Die Kommission kann Durchführungsrechtsakte erlassen, in denen die Art der Angaben, das Format und das Verfahren für Meldungen gemäß	(11) Die Kommission kann Durchführungsrechtsakte erlassen, in denen die Art der Angaben, das Format und das Verfahren für Meldungen gemäß

den Absätzen 1 und ***2*** näher bestimmt werden***. Die Kommission kann ferner Durchführungsrechtsakte erlassen, um genauer zu bestimmen, in welchen Fällen ein Sicherheitsvorfall als erheblich im Sinne des Absatzes 3 anzusehen ist***. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 37 Absatz 2 genannten Prüfverfahren erlassen.

Absatz 1 ***des vorliegenden Artikels*** und Artikel ***27*** näher bestimmt werden. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 37 Absatz 2 genannten Prüfverfahren erlassen.

Änderungsantrag 221

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 11 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(11a) Der Kommission wird die Befugnis übertragen, gemäß Artikel 36 delegierte Rechtsakte zu erlassen, um diese Richtlinie zu ergänzen, indem sie die Art der gemäß Absatz 1 des vorliegenden Artikels übermittelten Informationen festlegt und die Parameter näher bestimmt, die zu berücksichtigen sind, wenn bestimmt wird, ob ein Sicherheitsvorfall gemäß Absatz 3 dieses Artikels als erheblich gilt.

Änderungsantrag 222

Vorschlag für eine Richtlinie
Artikel 21 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Die Mitgliedstaaten ***können*** wesentliche und wichtige Einrichtungen ***dazu verpflichten***, bestimmte IKT-Produkte, -Dienste und -Prozesse im Rahmen ***spezifischer*** europäischer Systeme für die ***Cybersicherheitszertifizierung***, die gemäß Artikel 49 der Verordnung (EU) 2019/881 angenommen wurden, zertifizieren zu lassen, ***um die Erfüllung bestimmter in Artikel 18 genannter Anforderungen nachzuweisen. Die*** zu	(1) Die Mitgliedstaaten ***fordern*** wesentliche und wichtige Einrichtungen ***im Einklang mit den Leitlinien der ENISA, der Kommission und der Kooperationsgruppe auf***, bestimmte IKT-Produkte, -Dienste und -Prozesse***, die entweder von der wesentlichen oder wichtigen Einrichtung entwickelt oder von Dritten bezogen wurden,*** im Rahmen europäischer Systeme für die ***Cybersicherheit***, die gemäß Artikel 49 der

zertifizierenden Produkte, Dienstleistungen und Prozesse können von einer wesentlichen oder wichtigen Einrichtung entwickelt oder von Dritten beschafft worden sein.

Verordnung (EU) 2019/881 ***oder***, ***falls noch nicht verfügbar***, ***im Rahmen ähnlicher international anerkannter Zertifizierungsregelungen*** angenommen wurden, zertifizieren zu lassen***. Darüber hinaus fordern die Mitgliedstaaten wesentliche und wichtige Einrichtungen auf, qualifizierte Vertrauensdienste gemäß der Verordnung (EU) Nr. 910/2014 zu nutzen***.

Änderungsantrag 223

Vorschlag für eine Richtlinie
Artikel 21 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte zu erlassen, ***in denen*** ausgeführt wird, welche Kategorien wesentlicher Einrichtungen ein Zertifikat erlangen müssen und welche spezifischen europäischen Systeme für die ***Cybersicherheitszertifizierung*** dabei nach ***Absatz 1*** anzuwenden sind. ***Die*** delegierten Rechtsakte werden ***gemäß Artikel 36 erlassen***.	(2) Der Kommission wird die Befugnis übertragen, ***gemäß Artikel 36*** delegierte Rechtsakte zu erlassen, ***um diese Richtlinie dadurch zu ergänzen, dass*** ausgeführt wird, welche Kategorien wesentlicher ***und wichtiger*** Einrichtungen ein Zertifikat erlangen müssen und welche spezifischen europäischen Systeme für die ***Cybersicherheit*** dabei nach Artikel ***49 der Verordnung (EU) 2019/881*** anzuwenden sind. ***Solche*** delegierten Rechtsakte werden ***in Erwägung gezogen, wenn ein unzureichendes Niveau der Cybersicherheit festgestellt wurde; ihnen geht eine Folgenabschätzung voraus, und es wird eine Umsetzungsfrist vorgesehen***.

Änderungsantrag 224

Vorschlag für eine Richtlinie
Artikel 21 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Ist kein geeignetes europäisches System für die Cybersicherheitszertifizierung für die Zwecke des Absatzes 2 vorhanden, kann die Kommission die ENISA auffordern, ein vorläufiges System gemäß Artikel 48	(3) Ist kein geeignetes europäisches System für die Cybersicherheitszertifizierung für die Zwecke des Absatzes 2 vorhanden, kann die Kommission ***nach Konsultation der Kooperationsgruppe und der***

Absatz 2 der Verordnung (EU) 2019/881 auszuarbeiten.	***Europäischen Gruppe für die Cybersicherheitszertifizierung*** die ENISA auffordern, ein vorläufiges System gemäß Artikel 48 Absatz 2 der Verordnung (EU) 2019/881 auszuarbeiten.

Änderungsantrag 225

Vorschlag für eine Richtlinie
Artikel 22 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) In Zusammenarbeit mit den Mitgliedstaaten bietet die ENISA Beratung und erlässt Leitlinien zu den technischen Bereichen, die in Bezug auf Absatz 1 in Betracht zu ziehen sind, sowie zu den bereits bestehenden Normen – einschließlich der nationalen Normen der Mitgliedstaaten –, mit denen diese Bereiche abgedeckt werden könnten.	(2) In Zusammenarbeit mit den Mitgliedstaaten ***und gegebenenfalls nach Konsultation relevanter Interessenträger*** bietet die ENISA Beratung und erlässt Leitlinien zu den technischen Bereichen, die in Bezug auf Absatz 1 in Betracht zu ziehen sind, sowie zu den bereits bestehenden Normen – einschließlich der nationalen Normen der Mitgliedstaaten –, mit denen diese Bereiche abgedeckt werden könnten.

Änderungsantrag 226

Vorschlag für eine Richtlinie
Artikel 22 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
	(3) Die Kommission unterstützt und fördert in Zusammenarbeit mit der ENISA die Ausarbeitung und Durchsetzung von Normen, die von den einschlägigen Normungsgremien der Union sowie den internationalen Normungsgremien für die konvergente Umsetzung von Artikel 18 Absätze 1 und 2 festgelegt wurden. Die Kommission unterstützt die Aktualisierung der Normen im Lichte der technologischen Entwicklungen.

Änderungsantrag 227

Vorschlag für eine Richtlinie
Artikel 23 – Überschrift

Vorschlag der Kommission	*Geänderter Text*
Datenbanken der Domänennamen und Registrierungsdaten	***Datenbankstruktur*** der Domänennamen und Registrierungsdaten

Änderungsantrag 228

Vorschlag für eine Richtlinie
Artikel 23 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domänennamensystems zu leisten, ***stellen*** die Mitgliedstaaten ***sicher***, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste ***für die TLD*** erbringen, genaue und vollständige Domänennamen-Registrierungsdaten in einer ***eigenen Datenbank*** sammeln und pflegen, ***wobei*** die ***Datenschutzvorschriften der Union in Bezug auf personenbezogene Daten mit der gebotenen Sorgfalt zu beachten sind.***	(1) Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domänennamensystems zu leisten, ***schreiben*** die Mitgliedstaaten ***vor***, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, genaue***, überprüfte*** und vollständige Domänennamen-Registrierungsdaten in einer ***Datenbankstruktur*** sammeln und pflegen, die ***zu diesen Zwecken betrieben wird.***

Änderungsantrag 229

Vorschlag für eine Richtlinie
Artikel 23 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Mitgliedstaaten stellen sicher, dass die ***Datenbanken*** zu den in Absatz 1 genannten Domänennamen-Registrierungsdaten einschlägige Angaben ***enthalten***, anhand derer die Inhaber der Domänennamen und die Kontaktstellen, die die Domänennamen im Rahmen der TLD verwalten, identifiziert und kontaktiert werden können.	(2) Die Mitgliedstaaten stellen sicher, dass die ***Datenbankstruktur*** zu den in Absatz 1 genannten Domänennamen-Registrierungsdaten einschlägige Angaben ***enthält, die zumindest den Namen der Registranten***, ***ihre Anschrift, ihre E-Mail-Adresse und ihre Telefonnummer enthalten,*** anhand derer die Inhaber der Domänennamen und die Kontaktstellen, die die Domänennamen im Rahmen der TLD verwalten, identifiziert und kontaktiert werden können.

Änderungsantrag 230

Vorschlag für eine Richtlinie
Artikel 23 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, über Vorgaben und Verfahren verfügen, mit denen sichergestellt wird, dass die ***Datenbanken*** genaue und vollständige Angaben ***enthalten***. Die Mitgliedstaaten stellen sicher, dass diese Vorgaben und Verfahren öffentlich zugänglich gemacht werden.	(3) Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, über Vorgaben und Verfahren verfügen, mit denen sichergestellt wird, dass die ***Datenbankstruktur*** genaue***, überprüfte*** und vollständige Angaben ***enthält***. Die Mitgliedstaaten stellen sicher, dass diese Vorgaben und Verfahren öffentlich zugänglich gemacht werden.

Änderungsantrag 231

Vorschlag für eine Richtlinie
Artikel 23 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
(4) Die Mitgliedstaaten stellen sicher, dass die TLD-Register und ***die*** Einrichtungen, die Domänennamen-Registrierungsdienste ***für die TLD*** erbringen, unverzüglich nach der Registrierung eines Domänennamens die nicht personenbezogenen Domänenregistrierungsdaten ***veröffentlichen***.	(4) Die Mitgliedstaaten stellen sicher, dass die TLD-Register und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, unverzüglich nach der Registrierung eines Domänennamens die nicht personenbezogenen Domänenregistrierungsdaten ***öffentlich zugänglich machen. Wenn die Registranten juristische Personen sind, müssen die öffentlich zugänglichen Daten zur Domänenregistrierung mindestens den Namen des Registranten, seine physische Adresse, seine E-Mail-Adresse und seine Telefonnummer enthalten.***

Änderungsantrag 232

Vorschlag für eine Richtlinie
Artikel 23 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
(5) Die Mitgliedstaaten ***stellen sicher***, dass ***die*** TLD-Register und ***die*** Einrichtungen, die Domänennamen-Registrierungsdienste ***für die TLD*** erbringen, auf ***rechtmäßige und*** hinreichend begründete Anträge berechtigten Zugangsnachfragern im Einklang mit dem Datenschutzrecht der Union Zugang zu bestimmten Domänennamen-Registrierungsdaten gewähren. Die Mitgliedstaaten ***stellen sicher***, dass ***die*** TLD-Register und ***die*** Einrichtungen, die Domänennamen-Registrierungsdienste ***für die TLD*** erbringen, alle Anträge auf Zugang unverzüglich beantworten. Die Mitgliedstaaten stellen sicher, dass die Vorgaben und Verfahren für die Offenlegung solcher Daten öffentlich zugänglich gemacht werden.	(5) Die Mitgliedstaaten ***schreiben vor***, dass TLD-Register und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, auf hinreichend begründete Anträge berechtigten Zugangsnachfragern im Einklang mit dem Datenschutzrecht der Union Zugang zu bestimmten Domänennamen-Registrierungsdaten***, einschließlich personenbezogener Daten,*** gewähren. Die Mitgliedstaaten ***schreiben vor***, dass TLD-Register und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, alle Anträge auf Zugang unverzüglich ***und in jedem Fall innerhalb von 72 Stunden*** beantworten. Die Mitgliedstaaten stellen sicher, dass die Vorgaben und Verfahren für die Offenlegung solcher Daten öffentlich zugänglich gemacht werden.

Änderungsantrag 233

Vorschlag für eine Richtlinie
Artikel 24 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Für die Zwecke dieser Richtlinie wird davon ausgegangen, dass als Hauptniederlassung in der Union der in Absatz 1 genannten Einrichtungen jeweils die Niederlassung in demjenigen Mitgliedstaat gilt, in dem die Entscheidungen im Zusammenhang mit den Maßnahmen zum Cybersicherheitsrisikomanagement getroffen werden. Werden solche Entscheidungen in keiner Niederlassung in der Union getroffen, wird davon ausgegangen, dass sich die Hauptniederlassung der Einrichtung in dem Mitgliedstaat ***befindet***, in dem die Niederlassung mit der höchsten Beschäftigtenzahl in der Union angesiedelt	(2) Für die Zwecke dieser Richtlinie wird davon ausgegangen, dass als Hauptniederlassung in der Union der in Absatz 1 genannten Einrichtungen jeweils die Niederlassung in demjenigen Mitgliedstaat gilt, in dem die Entscheidungen im Zusammenhang mit den Maßnahmen zum Cybersicherheitsrisikomanagement getroffen werden. Werden solche Entscheidungen in keiner Niederlassung in der Union getroffen, wird davon ausgegangen, dass sich die Hauptniederlassung der Einrichtung ***entweder*** in dem Mitgliedstaat, in dem die Niederlassung mit der höchsten Beschäftigtenzahl in der Union angesiedelt ist***, oder in dem Mitgliedstaat befindet, in***

ist.	***dem die Niederlassung liegt, in der die Cybersicherheits-Operationen ausgeführt werden***

Änderungsantrag 234

Vorschlag für eine Richtlinie
Artikel 25 – Überschrift

Vorschlag der Kommission	*Geänderter Text*
Register ***wesentlicher und wichtiger Einrichtungen***	***ENISA-***Register

Änderungsantrag 235

Vorschlag für eine Richtlinie
Artikel 25 – Absatz 1 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(1) Die ENISA erstellt und pflegt ein Register wesentlicher und wichtiger Einrichtungen im Sinne des Artikels 24 Absatz 1***. Die Einrichtungen übermitteln der ENISA spätestens bis zum … [12 Monate nach Inkrafttreten der Richtlinie]*** folgende Angaben:	(1) Die ENISA erstellt und pflegt ein ***sicheres*** Register wesentlicher und wichtiger Einrichtungen im Sinne des Artikels 24 Absatz 1***, das*** folgende Angaben ***enthält***:

Änderungsantrag 236

Vorschlag für eine Richtlinie
Artikel 25 – Absatz 1 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) aktuelle Kontaktdaten, einschließlich E-Mail-Adressen ***und*** Telefonnummern der Einrichtungen.	c) aktuelle Kontaktdaten, einschließlich E-Mail-Adressen***, IP-Bereiche,*** Telefonnummern ***sowie relevanter Sektoren und Teilsektoren*** der Einrichtungen ***gemäß den Anhängen I und II***.

Änderungsantrag 237

Vorschlag für eine Richtlinie
Artikel 25 – Absatz 1 – Unterabsatz 1 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	Bis zum ... [12 Monate nach Inkrafttreten dieser Richtlinie] übermitteln die wesentlichen und wichtigen Einrichtungen die in Unterabsatz 1 genannten Informationen an die ENISA.

Änderungsantrag 238

Vorschlag für eine Richtlinie
Artikel 26 – Absatz 1 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(1) ***Unbeschadet der Verordnung (EU) 2016/679 stellen*** die Mitgliedstaaten sicher, dass wesentliche und wichtige Einrichtungen relevante Cybersicherheitsinformationen untereinander austauschen können, einschließlich Informationen über Cyberbedrohungen, Schwachstellen, Gefährdungsindikatoren (indicators of compromise – IoC), Taktiken, ***Techniken und Verfahren***, Cybersicherheitswarnungen und ***Konfigurationstools***, sofern	(1) Die Mitgliedstaaten ***stellen*** sicher, dass wesentliche und wichtige Einrichtungen ***und andere einschlägige Einrichtungen, die nicht in den Anwendungsbereich dieser Richtlinie fallen,*** relevante Cybersicherheitsinformationen untereinander austauschen können, einschließlich Informationen über Cyberbedrohungen, ***Beinahe-Vorfälle,*** Schwachstellen, ***Techniken und Verfahren, Metadaten und Inhaltsdaten,*** Gefährdungsindikatoren (indicators of compromise – IoC), ***gegnerische*** Taktiken, ***modi operandi, akteurspezifische Informationen***, Cybersicherheitswarnungen***, Taktiken der Industriespionage*** und ***empfohlene Konfigurationen für Sicherheitstools***, sofern

Änderungsantrag 239

Vorschlag für eine Richtlinie
Artikel 26 – Absatz 1 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) durch diesen Informationsaustausch das Cybersicherheitsniveau erhöht wird, insbesondere indem Aufklärungsarbeit über Cyberbedrohungen geleistet wird, die	b) durch diesen Informationsaustausch das Cybersicherheitsniveau erhöht wird, insbesondere indem Aufklärungsarbeit über Cyberbedrohungen geleistet wird, die

Fähigkeit solcher Bedrohungen, sich zu verbreiten eingedämmt bzw. verhindert wird und eine Reihe von Abwehrkapazitäten, die Beseitigung und Offenlegung von Schwachstellen, Techniken zur Erkennung von Bedrohungen, Eindämmungsstrategien ***oder*** Reaktions- und Wiederherstellungsphasen unterstützt werden.	Fähigkeit solcher Bedrohungen, sich zu verbreiten eingedämmt bzw. verhindert wird und eine Reihe von Abwehrkapazitäten, die Beseitigung und Offenlegung von Schwachstellen, Techniken zur Erkennung ***Eindämmung und Verhütung*** von Bedrohungen, Eindämmungsstrategien***,*** Reaktions- und Wiederherstellungsphasen unterstützt werden ***oder indem die gemeinsame Bedrohungsforschung zwischen öffentlichen und privaten Einrichtungen gefördert wird***.

Änderungsantrag 240

Vorschlag für eine Richtlinie
Artikel 26 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Mitgliedstaaten ***stellen sicher***, ***dass der*** Informationsaustausch ***innerhalb*** vertrauenswürdiger Gemeinschaften wesentlicher und wichtiger Einrichtungen ***stattfindet***. Dieser Austausch muss im Wege von Vereinbarungen über den Informationsaustausch unter Beachtung des potenziell sensiblen Charakters der ausgetauschten Informationen ***und im Einklang mit den in Absatz 1 genannten Vorschriften des Unionsrechts*** erfolgen.	(2) Die Mitgliedstaaten ***erleichtern den*** Informationsaustausch, ***indem sie die Einrichtung*** vertrauenswürdiger Gemeinschaften wesentlicher und wichtiger Einrichtungen ***und ihrer Diensteanbieter oder gegebenenfalls ihrer Lieferanten ermöglichen***. Dieser Austausch muss im Wege von Vereinbarungen über den Informationsaustausch unter Beachtung des potenziell sensiblen Charakters der ausgetauschten Informationen erfolgen.

Änderungsantrag 241

Vorschlag für eine Richtlinie
Artikel 26 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Die Mitgliedstaaten ***legen Vorschriften fest, in denen das Verfahren,*** die operativen Elemente (einschließlich der Nutzung spezieller IKT-Plattformen), ***der*** Inhalt ***und die Bedingungen*** der ***in Absatz 2 genannten Vereinbarungen über den Informationsaustausch bestimmt***	(3) Die Mitgliedstaaten ***erleichtern den Abschluss der in Absatz 2 genannten Vereinbarungen über den Informationsaustausch im Bereich der Cybersicherheit***, ***indem sie*** die operativen Elemente (einschließlich der Nutzung von speziellen IKT-Plattformen ***und***

werden. In diesen Vorschriften werden auch die Einzelheiten der Beteiligung von Behörden an solchen Vereinbarungen ***sowie operative Elemente, einschließlich der Nutzung spezieller IT-Plattformen, festgelegt***. Die Mitgliedstaaten unterstützen die Anwendung solcher Vereinbarungen im Einklang mit ihren in Artikel 5 Absatz 2 Buchstabe g genannten Konzepten.

Automatisierungswerkzeugen) und Inhalt ***zur Verfügung stellen. Die Mitgliedstaaten legen*** die Einzelheiten der Beteiligung von Behörden an solchen Vereinbarungen ***fest und können bestimmte Bedingungen für die von den zuständigen Behörden oder CSIRTs zur Verfügung gestellten Informationen vorschreiben***. Die Mitgliedstaaten unterstützen die Anwendung solcher Vereinbarungen im Einklang mit ihren in Artikel 5 Absatz 2 Buchstabe g genannten Konzepten.

Änderungsantrag 242

Vorschlag für eine Richtlinie
Artikel 27 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
Die Mitgliedstaaten stellen sicher, dass ***unbeschadet von Artikel 3 Einrichtungen, die nicht in den Anwendungsbereich dieser Richtlinie fallen,*** auf freiwilliger Basis ***erhebliche Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle melden können. Bei der Bearbeitung dieser Meldungen werden die Mitgliedstaaten gemäß dem in Artikel 20 vorgesehenen Verfahren tätig. Die Mitgliedstaaten können Pflichtmeldungen vorrangig vor freiwilligen Meldungen bearbeiten. Freiwillige Meldungen dürfen nicht dazu führen, dass der meldenden Einrichtung zusätzliche Verpflichtungen auferlegt werden, die nicht für sie gegolten hätten, wenn sie die Meldung nicht übermittelt hätte.***	Die Mitgliedstaaten stellen sicher, dass ***Meldungen dem CIRTS*** auf freiwilliger Basis ***übermittelt*** werden können ***von***

Änderungsantrag 243

Vorschlag für eine Richtlinie
Artikel 27 – Absatz 1 – Buchstabe a (neu)

Vorschlag der Kommission	*Geänderter Text*
	a) wesentlichen und wichtigen

	Einrichtungen in Bezug auf Cyberbedrohungen und Beinahe-Vorfälle;

Änderungsantrag 244

Vorschlag für eine Richtlinie
Artikel 27 – Absatz 1 – Buchstabe b (neu)

Vorschlag der Kommission	*Geänderter Text*
	b) Einrichtungen, die nicht in den Anwendungsbereich dieser Richtlinie fallen, in Bezug auf erhebliche Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle.

Änderungsantrag 245

Vorschlag für eine Richtlinie
Artikel 27 – Absatz 1 – Unterabsatz 1 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	Bei der Bearbeitung dieser Meldungen werden die Mitgliedstaaten gemäß dem in Artikel 20 vorgesehenen Verfahren tätig. Die Mitgliedstaaten können Pflichtmeldungen vorrangig vor freiwilligen Meldungen bearbeiten. Erforderlichenfalls übermitteln die CSIRTs der zentralen Anlaufstelle und gegebenenfalls den zuständigen Behörden die Informationen über die gemäß diesem Artikel eingegangenen Meldungen, wobei sie die Vertraulichkeit und den angemessenen Schutz der von der meldenden Einrichtung übermittelten Informationen sicherstellen. Freiwillige Meldungen dürfen nicht dazu führen, dass der meldenden Einrichtung zusätzliche Verpflichtungen auferlegt werden, die nicht für sie gegolten hätten, wenn sie die Meldung nicht übermittelt hätte.

Änderungsantrag 246

Vorschlag für eine Richtlinie
Artikel 28 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Bei der Bearbeitung von Sicherheitsvorfällen, die zur Verletzung des Schutzes personenbezogener Daten führen, arbeiten die zuständigen Behörden eng mit den Datenschutzbehörden zusammen.	(2) Bei der Bearbeitung von Sicherheitsvorfällen, die zur Verletzung des Schutzes personenbezogener Daten führen, arbeiten die zuständigen Behörden eng mit den Datenschutzbehörden zusammen. ***Dies geschieht im Einklang mit ihrer Zuständigkeit und ihren Aufgaben gemäß der Verordnung (EU) 2016/679.***

Änderungsantrag 247

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 2 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) Vor-Ort-Kontrollen und externe Aufsichtsmaßnahmen, einschließlich Stichprobenkontrollen;	a) Vor-Ort-Kontrollen und externe Aufsichtsmaßnahmen, einschließlich ***von geschulten Fachleuten durchgeführten*** Stichprobenkontrollen;

Änderungsantrag 248

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 2 – Buchstabe a a (neu)

Vorschlag der Kommission	*Geänderter Text*
	aa) Untersuchung von Fällen der Nichteinhaltung und deren Auswirkungen auf die Sicherheit der Dienste;

Änderungsantrag 249

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 2 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) ***regelmäßige Prüfungen***;	b) ***jährliche und gezielte Sicherheitsprüfungen, die von einer***

	qualifizierten unabhängigen Stelle oder einer zuständigen Behörde durchgeführt werden;

Änderungsantrag 250

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 2 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) ***gezielte Sicherheitsprüfungen auf der Grundlage von Risikobewertungen*** oder ***verfügbaren risikobezogenen Informationen***;	c) ***Ad-hoc-Prüfung in Fällen, die aufgrund eines erheblichen Sicherheitsvorfalls*** oder ***Verstoßes der wesentlichen Einrichtung gerechtfertigt sind***;

Änderungsantrag 251

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 2 – Unterabsätze 1 a und 1 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	Die in Unterabsatz 1 Buchstabe b genannten gezielten Sicherheitsprüfungen stützen sich auf Risikobewertungen, die von der zuständigen Behörde oder der geprüften Einrichtung durchgeführt werden, oder auf andere risikobezogene verfügbare Informationen.
	Die Ergebnisse einer gezielten Sicherheitsprüfung sind der zuständigen Behörde zur Verfügung zu stellen. Die Kosten einer solchen gezielten Sicherheitsprüfung, die von einer qualifizierten unabhängigen Stelle durchgeführt wird, sind von der betreffenden Einrichtung zu tragen.

Änderungsantrag 252

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 2 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(2a) Wenn die zuständigen Behörden ihre Befugnisse gemäß Absatz 2 Buchstaben a bis d ausüben, müssen sie die Auswirkungen auf die Unternehmensprozesse der Einrichtung so gering wie möglich halten.

Änderungsantrag 253

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 4 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) verbindliche Anweisungen oder Anordnungen zu ***erteilen***, um diese Einrichtungen aufzufordern, die festgestellten Mängel oder die Verstöße gegen die in dieser Richtlinie festgelegten Verpflichtungen zu beheben;	b) verbindliche Anweisungen ***zu erteilen, auch in Bezug auf Maßnahmen, die zur Verhütung oder Behebung eines Sicherheitsvorfalls erforderlich sind, sowie Fristen für die Durchführung dieser Maßnahmen und für die Berichterstattung über ihre Durchführung zu setzen,*** oder Anordnungen zu ***erlassen***, um diese Einrichtungen aufzufordern, die festgestellten Mängel oder die Verstöße gegen die in dieser Richtlinie festgelegten Verpflichtungen zu beheben;

Änderungsantrag 254

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 4 – Buchstabe i

Vorschlag der Kommission	*Geänderter Text*
i) eine öffentliche Erklärung abzugeben, in der die Art des Verstoßes sowie die juristische(n) und natürliche(n) Person(en) genannt wird bzw. werden, die für den Verstoß gegen eine in dieser Richtlinie festgelegte Verpflichtung verantwortlich ist bzw. sind;	***entfällt***

Änderungsantrag 255

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 4 – Buchstabe j

Vorschlag der Kommission	*Geänderter Text*
j) ***je nach den*** einzelstaatlichen ***Rechtsvorschriften*** und den Umständen des Einzelfalls zusätzlich zu den ***oder anstelle der*** unter den Buchstaben a bis i dieses Absatzes genannten Maßnahmen eine Geldbuße gemäß Artikel 31 zu verhängen oder die zuständigen Stellen oder Gerichte um die Verhängung einer solchen Geldbuße zu ersuchen.	j) ***gemäß dem*** einzelstaatlichen ***Recht*** und den Umständen des Einzelfalls zusätzlich zu den unter den Buchstaben a bis i dieses Absatzes genannten Maßnahmen eine Geldbuße gemäß Artikel 31 zu verhängen oder die zuständigen Stellen oder Gerichte um die Verhängung einer solchen Geldbuße zu ersuchen.

Änderungsantrag 256

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 5 – Unterabsatz 1 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) die Zertifizierung oder Genehmigung für einen Teil oder alle von einer wesentlichen Einrichtung erbrachten Dienste oder Tätigkeiten auszusetzen oder eine Zertifizierungs- oder Genehmigungsstelle aufzufordern, die Zertifizierung oder Genehmigung auszusetzen;	a) die Zertifizierung oder Genehmigung für einen Teil oder alle von einer wesentlichen Einrichtung erbrachten ***einschlägigen*** Dienste oder Tätigkeiten auszusetzen oder eine Zertifizierungs- oder Genehmigungsstelle aufzufordern, die Zertifizierung oder Genehmigung ***vorübergehend*** auszusetzen;

Änderungsantrag 257

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 5 – Unterabsatz 1 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) ***gegen Personen, die auf Geschäftsführungs- bzw. Vorstandsebene*** oder ***Ebene des rechtlichen Vertreters*** Leitungsaufgaben in dieser ***wesentlichen*** Einrichtung ***wahrnehmen, und gegen jede andere natürliche Person***, die ***für den Verstoß Verantwortung trägt, ein vorübergehendes Verbot zur Wahrnehmung von*** Leitungsaufgaben in dieser Einrichtung ***zu verhängen oder von***	b) ***als äußerstes Mittel von den zuständigen Stellen*** oder ***Gerichten die Verhängung eines vorübergehenden Verbots zur Wahrnehmung von*** Leitungsaufgaben in dieser Einrichtung ***gemäß nationalem Recht gegen Personen***, die ***auf Geschäftsführungs- bzw. Vorstandsebene oder Ebene des rechtlichen Vertreters*** Leitungsaufgaben in dieser ***wesentlichen*** Einrichtung

den zuständigen Stellen oder Gerichten die Verhängung eines solchen Verbots zu verlangen.

wahrnehmen, zu verlangen.

Änderungsantrag 258

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 5 – Unterabsatz 2

Vorschlag der Kommission	*Geänderter Text*
Diese Sanktionen werden nur so lange angewandt, bis die Einrichtung die erforderlichen Maßnahmen ergreift, um die Mängel zu beheben oder die Anforderungen der zuständigen Behörde, wegen deren Nichterfüllung die Sanktionen verhängt wurden, zu erfüllen.	***Vorübergehende Aussetzungen oder Verbote nach diesem Absatz*** werden nur so lange angewandt, bis die ***betreffende*** Einrichtung die erforderlichen Maßnahmen ergreift, um die Mängel zu beheben oder die Anforderungen der zuständigen Behörde, wegen deren Nichterfüllung die Sanktionen verhängt wurden, zu erfüllen. ***Für die Anwendung solcher vorübergehenden Aussetzungen oder Verbote muss es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, der Unschuldsvermutung und des Rechts auf Verteidigung, entsprechen.***

Änderungsantrag 259

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 7 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) die Höhe des ***tatsächlich*** entstandenen Schadens ***bzw. entstandener Verluste oder potenzieller Schäden oder Verluste***, ***die hätten verursacht werden können, sofern sich diese feststellen lassen. Bei der Bewertung dieses Aspekts sind unter anderem tatsächliche oder potenzielle*** finanzielle oder wirtschaftliche Verluste, Auswirkungen auf andere Dienste sowie die Zahl der betroffenen ***oder potenziell betroffenen*** Nutzer ***zu***	c) die Höhe des entstandenen Schadens, ***darunter*** finanzielle oder wirtschaftliche Verluste, Auswirkungen auf andere Dienste sowie die Zahl der betroffenen Nutzer;

berücksichtigen;

Änderungsantrag 260

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 7 – Buchstabe c a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ca) alle einschlägigen früheren Verstöße der betroffenen Einrichtung;

Änderungsantrag 261

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 9

Vorschlag der Kommission	*Geänderter Text*
(9) Die Mitgliedstaaten stellen sicher, dass ihre zuständigen Behörden bei der Ausübung ihrer Aufsichts- und Durchsetzungsbefugnisse, mit denen sichergestellt werden soll, dass wesentliche Einrichtungen, die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] als kritische Einrichtungen oder als einer kritischen Einrichtung gleichgestellte Einrichtungen eingestuft wurden, die Verpflichtungen aus dieser Richtlinie erfüllen, die jeweils zuständigen Behörden ***des betreffenden Mitgliedstaats***, die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannt wurden, unterrichten. Auf Ersuchen von gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] zuständigen Behörden dürfen die zuständigen Behörden ihre Aufsichts- und Durchsetzungsbefugnisse in Bezug auf eine als kritisch oder als einer kritischen Einrichtung gleichwertig eingestufte wesentliche Einrichtung ausüben.	(9) Die Mitgliedstaaten stellen sicher, dass ihre zuständigen Behörden bei der Ausübung ihrer Aufsichts- und Durchsetzungsbefugnisse, mit denen sichergestellt werden soll, dass wesentliche Einrichtungen, die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] als kritische Einrichtungen oder als einer kritischen Einrichtung gleichgestellte Einrichtungen eingestuft wurden, die Verpflichtungen aus dieser Richtlinie erfüllen, die jeweils zuständigen Behörden ***aller betroffenen Mitgliedstaaten***, die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannt wurden, unterrichten. Auf Ersuchen von gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] zuständigen Behörden dürfen die zuständigen Behörden ihre Aufsichts- und Durchsetzungsbefugnisse in Bezug auf eine als kritisch oder als einer kritischen Einrichtung gleichwertig eingestufte wesentliche Einrichtung ausüben.

Änderungsantrag 262

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 9 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(9a) Die Mitgliedstaaten stellen sicher, dass ihre zuständigen Behörden mit den gemäß der Verordnung (EU) XXXX/XXXX [DORA] benannten einschlägigen zuständigen Behörden des betreffenden Mitgliedstaats zusammenarbeiten.

Änderungsantrag 263

Vorschlag für eine Richtlinie
Artikel 30 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Werden Nachweise oder Hinweise dafür vorgelegt, dass eine wichtige Einrichtung ihren Verpflichtungen nach dieser Richtlinie, insbesondere den Artikeln 18 und 20, nicht nachkommt, so stellen die Mitgliedstaaten sicher, dass die zuständigen Behörden erforderlichenfalls im Wege von nachträglichen Aufsichtsmaßnahmen tätig werden.	(1) Werden Nachweise oder Hinweise dafür vorgelegt, dass eine wichtige Einrichtung ihren Verpflichtungen nach dieser Richtlinie, insbesondere den Artikeln 18 und 20, nicht nachkommt, so stellen die Mitgliedstaaten sicher, dass die zuständigen Behörden erforderlichenfalls im Wege von nachträglichen Aufsichtsmaßnahmen tätig werden. ***Die Mitgliedstaaten stellen sicher, dass diese Maßnahmen wirksam, verhältnismäßig und abschreckend sind, wobei die Umstände jedes einzelnen Falls zu berücksichtigen sind.***

Änderungsantrag 264

Vorschlag für eine Richtlinie
Artikel 30 – Absatz 2 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) Vor-Ort-Kontrollen und nachträgliche externe Aufsichtsmaßnahmen;	a) Vor-Ort-Kontrollen und nachträgliche externe Aufsichtsmaßnahmen***, die von geschulten Fachleuten durchgeführt werden***;

Änderungsantrag 265

Vorschlag für eine Richtlinie
Artikel 30 – Absatz 2 – Buchstabe a a (neu)

Vorschlag der Kommission	*Geänderter Text*
	aa) Untersuchung von Fällen der Nichteinhaltung und deren Auswirkungen auf die Sicherheit der Dienste;

Änderungsantrag 266

Vorschlag für eine Richtlinie
Artikel 30 – Absatz 2 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) gezielte Sicherheitsprüfungen ***auf der Grundlage von Risikobewertungen*** oder ***verfügbaren risikobezogenen Informationen***;	b) gezielte Sicherheitsprüfungen***, die von einer qualifizierten unabhängigen Stelle*** oder ***einer zuständigen Behörde durchgeführt werden***;

Änderungsantrag 267

Vorschlag für eine Richtlinie
Artikel 30 – Absatz 2 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) Sicherheitsscans auf der Grundlage objektiver, fairer und transparenter Risikobewertungskriterien;	c) Sicherheitsscans auf der Grundlage objektiver, ***nichtdiskriminierender,*** fairer und transparenter Risikobewertungskriterien;

Änderungsantrag 268

Vorschlag für eine Richtlinie
Artikel 30 – Absatz 2 – Unterabsätze 1 a und 1 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	Die in Unterabsatz 1 Buchstabe b genannten gezielten Sicherheitsprüfungen stützen sich auf Risikobewertungen, die von der zuständigen Behörde oder der geprüften

	Einrichtung durchgeführt werden, oder auf andere risikobezogene verfügbare Informationen.
	Die Ergebnisse einer gezielten Sicherheitsprüfung sind der zuständigen Behörde zur Verfügung zu stellen. Die Kosten einer solchen gezielten Sicherheitsprüfung, die von einer qualifizierten unabhängigen Stelle durchgeführt wird, sind von der betreffenden Einrichtung zu tragen.

Änderungsantrag 269

Vorschlag für eine Richtlinie
Artikel 30 – Absatz 4 – Buchstabe h

Vorschlag der Kommission	*Geänderter Text*
h) eine öffentliche Erklärung abzugeben, in der die Art des Verstoßes sowie die juristische(n) und natürliche(n) Person(en) genannt wird bzw. werden, die für den Verstoß gegen eine in dieser Richtlinie festgelegte Verpflichtung verantwortlich ist bzw. sind;	***entfällt***

Änderungsantrag 270

Vorschlag für eine Richtlinie
Artikel 30 – Absatz 4 – Buchstabe i

Vorschlag der Kommission	*Geänderter Text*
i) ***je nach den einzelstaatlichen Rechtsvorschriften*** und den Umständen des Einzelfalls zusätzlich zu den ***oder anstelle der*** unter den Buchstaben a bis h dieses Absatzes genannten Maßnahmen eine Geldbuße gemäß Artikel 31 zu verhängen oder die zuständigen Stellen oder Gerichte um die Verhängung einer solchen Geldbuße zu ersuchen.	i) ***gemäß einzelstaatlichem Recht*** und den Umständen des Einzelfalls zusätzlich zu den unter den Buchstaben a bis h dieses Absatzes genannten Maßnahmen eine Geldbuße gemäß Artikel 31 zu verhängen oder die zuständigen Stellen oder Gerichte um die Verhängung einer solchen Geldbuße zu ersuchen.

Änderungsantrag 271

Vorschlag für eine Richtlinie
Artikel 31 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu ***oder anstelle von*** Maßnahmen nach Artikel 29 Absatz 4 Buchstaben a bis i, Artikel 29 Absatz 5 und Artikel 30 Absatz 4 Buchstaben a bis h verhängt.	(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu Maßnahmen nach Artikel 29 Absatz 4 Buchstaben a bis i, Artikel 29 Absatz 5 und Artikel 30 Absatz 4 Buchstaben a bis h verhängt.

Änderungsantrag 272

Vorschlag für eine Richtlinie
Artikel 32 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Haben die zuständigen Behörden Hinweise darauf, dass der Verstoß einer wesentlichen oder wichtigen Einrichtung gegen die in den Artikeln 18 und 20 festgelegten Verpflichtungen eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 ***Absatz*** 12 der Verordnung (EU) 2016/679 zur Folge hat, die gemäß Artikel 33 der genannten Verordnung zu melden ist, unterrichten sie die gemäß den Artikeln 55 und 56 jener Verordnung zuständigen Aufsichtsbehörden innerhalb ***einer angemessenen Frist***.	(1) Haben die zuständigen Behörden Hinweise darauf, dass der Verstoß einer wesentlichen oder wichtigen Einrichtung gegen die in den Artikeln 18 und 20 festgelegten Verpflichtungen eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 ***Nummer*** 12 der Verordnung (EU) 2016/679 zur Folge hat, die gemäß Artikel 33 der genannten Verordnung zu melden ist, unterrichten sie die gemäß den Artikeln 55 und 56 jener Verordnung zuständigen Aufsichtsbehörden ***unverzüglich und in jedem Fall innerhalb von 72 Stunden, nachdem sie Kenntnis von der Verletzung des Schutzes personenbezogener Daten erlangt haben***.

Änderungsantrag 273

Vorschlag für eine Richtlinie
Artikel 32 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Ist die gemäß der Verordnung (EU) 2016/679 zuständige Aufsichtsbehörde in einem anderen Mitgliedstaat angesiedelt als die zuständige Behörde, so ***kann*** die zuständige Behörde die im selben	(3) Ist die gemäß der Verordnung (EU) 2016/679 zuständige Aufsichtsbehörde in einem anderen Mitgliedstaat angesiedelt als die zuständige Behörde, so ***setzt*** die zuständige Behörde die im selben

Mitgliedstaat angesiedelte Aufsichtsbehörde davon in Kenntnis ***setzen***.	Mitgliedstaat angesiedelte Aufsichtsbehörde davon in Kenntnis.

Änderungsantrag 274

Vorschlag für eine Richtlinie
Artikel 35 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
Die Kommission überprüft regelmäßig die Anwendung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat Bericht. In dem Bericht wird insbesondere die Relevanz der in den Anhängen I und II genannten Sektoren, Teilsektoren und Einrichtungen unterschiedlicher Größe und Art für das Funktionieren der Wirtschaft und Gesellschaft in Bezug auf die Cybersicherheit bewertet. Zu diesem Zweck berücksichtigt die Kommission im Hinblick auf die weitere Förderung der strategischen und operativen Zusammenarbeit die Berichte der Kooperationsgruppe und des CSIRT-Netzwerks über die auf strategischer und operativer Ebene gemachten Erfahrungen. ***Der erste Bericht dieser Art ist bis zum … [54 Monate nach Inkrafttreten dieser Richtlinie] vorzulegen.***	***Bis zum … [42 Monate nach dem Tag des Inkrafttretens dieser Richtlinie] und danach alle 36 Monate*** überprüft ***die Kommission*** regelmäßig die Anwendung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat ***darüber*** Bericht. In dem Bericht wird insbesondere die Relevanz der in den Anhängen I und II genannten Sektoren, Teilsektoren und Einrichtungen unterschiedlicher Größe und Art für das Funktionieren der Wirtschaft und Gesellschaft in Bezug auf die Cybersicherheit bewertet. Zu diesem Zweck berücksichtigt die Kommission im Hinblick auf die weitere Förderung der strategischen und operativen Zusammenarbeit die Berichte der Kooperationsgruppe und des CSIRT-Netzwerks über die auf strategischer und operativer Ebene gemachten Erfahrungen. ***Dem Bericht wird erforderlichenfalls ein Gesetzgebungsvorschlag beigefügt.***

Änderungsantrag 275

Vorschlag für eine Richtlinie
Artikel 36 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 18 Absatz 6 und Artikel 21 Absatz 2 wird der Kommission für einen Zeitraum von fünf Jahren ab dem […] übertragen.	(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 18 Absatz 6***, Artikel 20 Absatz 11a*** und Artikel 21 Absatz 2 wird der Kommission für einen Zeitraum von fünf Jahren ab dem

[…] übertragen.

Änderungsantrag 276

Vorschlag für eine Richtlinie
Artikel 36 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Die Befugnisübertragung gemäß Artikel 18 Absatz 6 und Artikel 21 Absatz 2 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.	(3) Die Befugnisübertragung gemäß Artikel 18 Absatz 6***, Artikel 20 Absatz 11a*** und Artikel 21 Absatz 2 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

Änderungsantrag 277

Vorschlag für eine Richtlinie
Artikel 36 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
(6) Ein delegierter Rechtsakt, der gemäß Artikel 18 Absatz 6 und Artikel 21 Absatz 2 erlassen wurde, tritt 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 erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.	(6) Ein delegierter Rechtsakt, der gemäß Artikel 18 Absatz 6***, Artikel 20 Absatz 11a*** und Artikel 21 Absatz 2 erlassen wurde, tritt 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 erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.

Änderungsantrag 278

Vorschlag für eine Richtlinie
Artikel 42 – Absatz 1a (neu)

Vorschlag der Kommission	*Geänderter Text*
	Die Artikel 39 und 40 gelten jedoch ab dem … [18 Monate nach Inkrafttreten dieser Richtlinie].

Änderungsantrag 279

Vorschlag für eine Richtlinie
Anhang I – Nummer 2 – Buchstabe d – Spiegelstrich 2 (neu)

Vorschlag der Kommission

Geänderter Text

2. Verkehr	d) Straßenverkehr	– ***Betreiber von intelligenten Ladediensten für Elektrofahrzeuge***

Änderungsantrag 280

Vorschlag für eine Richtlinie
Anhang II – Tabelle – Zeile 6 a (neu)

Vorschlag der Kommission

Geänderter Text

6a. Bildung und Forschung		***– Hochschuleinrichtungen und Forschungsinstitute***

BEGRÜNDUNG

Der Berichterstatter möchte, dass Europa der beste Ort zum Leben und zur Abwicklung von

Geschäften wird.

Der Berichterstatter begrüßt daher die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2), die die ursprüngliche NIS-Richtlinie (NIS1) ersetzt. In dem Vorschlag spiegelt sich die veränderte Bedrohungslage im Bereich der Cybersicherheit wider und es wird eine Mindestharmonisierung der Maßnahmen in der EU eingeführt.

Heutzutage fällt es den europäischen Polizeikräften zunehmend schwerer, mit dem steilen Anstieg von Cybercrime-Vorfällen fertig zu werden. Dazu können High-Tech-Kriminalität, durch den Cyberspace ermöglichte Kriminalität und CEO-Betrug gehören, aber der Berichterstatter möchte ausdrücklich auf den aggressiven Anstieg von Ransomware-Banden hinweisen, die europäische Ziele unabhängig von deren Größe oder Umsatz hacken und erpressen. Auf der anderen Seite konzentrieren sich gegnerische nationalstaatliche Akteure auf den Diebstahl geistigen Eigentums in industriellem Maßstab, was eine entsprechende Antwort erfordert.

Laut ENISA sind die allgemeinen Ausgaben für Cybersicherheit bei Organisationen in der EU jedoch um 41 % niedriger als in den USA. Darüber hinaus wurde der Informationsaustausch zwischen Ländern und innerhalb von Ländern aufgrund von DSGVO-Haftungsängsten stark behindert. Dies zeigt sich sowohl bei öffentlichen als auch bei privaten Einrichtungen, die sich davor scheuen, Daten zu teilen. In der NIS2 muss daher deutlich festgelegt werden, dass der Informationsaustausch eine wesentliche Voraussetzung für die Erfüllung der Anforderungen an die Cybersicherheit ist.

Ein gemeinsames Niveau an Cybersicherheit in der EU ist entscheidend für das Funktionieren des Binnenmarkts. Eine klar definierte Gesetzgebung ist notwendig, damit Unternehmen, die in verschiedenen Mitgliedstaaten tätig sind, den gleichen Regeln unterworfen sind. Ziel der NIS2 ist es, die Unsicherheit und den derzeitigen Mangel an Klarheit zu beseitigen.

In einer Zeit, in der Cyberkriminalität, Spionage- oder Sabotageaktionen kaskadenartige Auswirkungen haben können, wird der Anwendungsbereich der NIS2 zu Recht erheblich erweitert. Der Vorschlag umfasst Bereiche, die bisher nicht als essentiell oder wichtig angesehen wurden, aber von Ransomware-Banden oder bestimmten Nationalstaaten definitiv als solche betrachtet werden. Basierend auf den Dienstleistungen, die Einrichtungen für Gesellschaften erbringen, werden diese in die folgenden zwei rechtlichen Kategorien unterteilt: „wesentliche“ und „wichtige“ Einrichtungen. Der Berichterstatter teilt die Ambition des Vorschlags der Kommission und ist der Ansicht, dass Forschungs- und akademische Einrichtungen als neuer Sektor aufgenommen werden sollten. Diese Einrichtungen sind stark betroffen, und ihr geistiges Eigentum verdient den Schutz durch die NIS2.

Die administrative Belastung und der bürokratische Aufwand für Unternehmen muss allen Gesetzgebern ein ständiges Anliegen sein. Der Berichterstatter befürwortet den Ausschluss von Kleinst- und Kleinunternehmen. Außerdem ist er der Meinung, dass sich die NIS2 nicht nur auf die Einhaltung von Vorschriften und strafrechtliche Maßnahmen konzentrieren sollte, sondern auch auf positive Anreize, wie z. B. die Bereitstellung von Beratung und Unterstützung für KMU, die spezielle Bedürfnisse und Interessen haben, oder auf kostenlos angebotene Dienste zur Überprüfung der E-Mail-Server- und Website-Konfiguration. Solche Vorschläge sollen auch in diesem Zusammenhang verdeutlichen, dass Regierungen dienstleistungsorientiert sein müssen.

Die **Meldepflicht für Sicherheitsvorfälle** ist für die Cybersicherheit entscheidend: Dadurch kann verhindert werden, dass andere Opfer eines Cyberangriffs werden. Der Berichterstatter

möchte anmerken, dass es ihm in seiner früheren Tätigkeit im Bereich der Cybersicherheit oft unmöglich war, einen Sicherheitsvorfall innerhalb von 24 Stunden zu melden. Normalerweise ist ein Sicherheitsvorfall in diesem frühen Stadium noch unklar und wird erst später aufgeklärt. Dem Berichterstatter erscheint der vorgeschlagene Zeitrahmen von 24 Stunden unangemessen, auch aufgrund der Tatsache, dass die Bemühungen der Experten vorerst auf eine Entschärfung des Problems ausgerichtet sind; die Berichterstattung ist in diesem Stadium von untergeordnetem Interesse. Der Cybervorfall und seine Auswirkungen werden innerhalb von 24 Stunden selten gut verstanden, und Meldungen innerhalb von 24 Stunden könnten zu falschen Meldungen, Übermeldungen und weiterer Verwirrung führen. Zudem ereignen sich diese Vorfälle oft am Wochenende. Daher schlägt der Berichterstatter vor, diese Richtlinie an anderes Unionsrecht, wie die DSGVO, anzugleichen und die Frist auf 72 Stunden zu erhöhen.

Der Berichterstatter hält es nicht für wünschenswert, die **Meldung potenzieller Vorfälle** verbindlich vorzuschreiben. Die freiwillige Mitteilung potenzieller Vorfälle oder Beinahe-Vorfälle sollte gefördert werden, aber mittlere und große Einrichtungen können potenziell Dutzende oder sogar Hunderte von bedeutenden Cyber-Bedrohungen an einem einzigen Tag haben. Die Meldung dieser potenziellen Vorfälle wäre aufwändig und würde die Wirksamkeit der Reaktion beeinträchtigen. Es könnte auch die Wirksamkeit der Behörden beeinträchtigen, die sich mit diesen Meldungen befassen müssen, da das Vertrauen in das Meldesystem und ihre Fähigkeit, auf tatsächliche Vorfälle zu reagieren, untergraben würde.

Auch die **Meldung potenzieller Cyber-Bedrohungen** an CSIRTs oder zuständige Behörden sollte nicht obligatorisch sein. Einhaltung von Vorschriften und Haftung werden die Aktivitäten von Bedrohungsjägern entmutigen; ein wesentlicher Teil des Ökosystems der Cybersicherheit. Darüber hinaus gibt es (schwerwiegende) Anlässe, bei denen es besser wäre, eine Bedrohung an die Sicherheitsdienste zu melden, wenn sie in deren Zuständigkeitsbereich liegt, anstatt an die NIS-Behörden.

Cybersicherheitsmaßnahmen sollten der Größe der Einrichtung und den Cybersicherheitsrisiken, denen sie ausgesetzt ist, entsprechen. Daher sollte die **Überwachung und Durchsetzung** verhältnismäßig sein. Zwar sind die Bußgelder und strafrechtlichen Maßnahmen unerlässlich, wenn die NIS2-Gesetzgebung wirksam sein soll, aber der Berichterstatter ist der Meinung, dass der Gesetzgeber betonen sollte, dass es eine „Eskalationsleiter“ gibt und die Geschäftsleitung erst nach nachweislicher Fahrlässigkeit bei wiederholten Warnungen bereit sein sollte, die Kraft des Gesetzes zu spüren. Die **Verhinderung einer doppelten Aufsicht** durch sektorspezifische Gesetzgebung ist auch für Einrichtungen wichtig, die sowohl in den Anwendungsbereich der NIS2 als auch in den einer sektorspezifischen Gesetzgebung, wie z. B. DORA, fallen.

Der Berichterstatter ermutigt alle Mitgliedstaaten, eine **nationale Cybersicherheitsstrategie zur aktiven Cyberverteidigung** zu formulieren. In Europa sind wir gut darin geworden, uns zu koordinieren, nachdem ein Sicherheitsvorfall eingetreten ist, aber die Zunahme des öffentlichen und privaten Wissens über Cyberangriffe, bevor sie eintreten, bringt auch eine Verantwortung mit sich. Es reicht nicht aus, dieses Wissen nur passiv zu teilen; Bürger und Einrichtungen erwarten von ihren Regierungen eine aktive Haltung in Bezug auf den Schutz der Cybersicherheit. Die Mitgliedstaaten müssen Fähigkeiten entwickeln, um Angriffe zu verhindern und ihnen aktiv vorzubeugen.

Auch der **Kern des Internets** braucht Aufmerksamkeit. Die DNS-Dienste müssen den Kunden sichere und datenschutzkonforme Dienste anbieten. Dies wird noch nicht allgemein akzeptiert. Der Berichterstatter ist darüber besorgt, dass Bürger, die ihren eigenen DNS-Dienst auf einem Laptop oder einem kleinen Server zu Hause haben, in den

Anwendungsbereich des Kommissionsvorschlags fallen. Der Berichterstatter wünscht, dass diese Personen, bei denen es sich häufig um technisch versierte Personen handelt, von dieser Richtlinie ausgenommen werden. Ein weiteres Problem ist, dass Betreiber von Root-Namenservern in den Geltungsbereich des NIS2 mit einbezogen werden. Seitdem sich das Internet in den 1970er, 1980er Jahren und darüber hinaus entwickelt hat, werden diese Dienste von guten Experten ehrenamtlich betrieben. Da dieser Dienst nicht monetarisiert wird und man argumentieren kann, dass Regierungen ihn nicht regulieren sollten, ist der Berichterstatter der Ansicht, dass Root-Server **vom Anwendungsbereich ausgenommen** werden sollten.

Der Berichterstatter hält es für äußerst wichtig, die Sicherheit von elektronischen Kommunikationsnetzen und -diensten insgesamt zu stärken und die Integrität des Internets zu verbessern. Das bedeutet, dass europaweit interoperable Vertrauensverfahren eingesetzt werden sollten. Europäische DNS-Resolver mit besonderem Augenmerk auf Datenschutz und Sicherheit werden stark gefördert, ebenso wie der physische Schutz von Internet-Backbone- und Unterseekommunikationskabeln. Diese Richtlinie sollte daher im Kontext des Gesamtpakets der Cybersicherheitsstrategie gesehen werden, die von der Kommission auf den Weg gebracht wurde: wir brauchen einen sichereren Internet-Kern.

Darüber hinaus bietet die NIS2 die rechtliche Grundlage für **koordinierte Sicherheitsrisikobewertungen** durch die Kooperationsgruppe. Die 5G-Toolbox dient als hervorragendes Beispiel dafür. Der Berichterstatter ist der Ansicht, dass diese Risikobewertungen die Sicherheit und die strategische Souveränität der Union erheblich verbessern könnten, und ist der Meinung, dass diese Risikobewertungen für eine breite Palette von IKT-Diensten, -Systemen oder -Produkten durchgeführt werden sollten. Frachtkontrollsysteme in Flughäfen und Häfen sind ein explizites Beispiel, das er in diesem Zusammenhang nennen möchte.

Ein wichtiger Informationsaustausch wird unbeabsichtigt stark behindert und sollte verbessert werden. Ein Beispiel: In den vergangenen Jahren haben Polizeikräfte Server von Ransomware-Banden mit teilweise Millionen von Opfern in und außerhalb der EU entdeckt und entschlüsselt. Die Aufgabe der Polizei ist es, an neuen Fällen zu arbeiten, so dass die CSIRT mit den aufgedeckten Informationen auf diesen Servern die Ziele erreichen und die Cyber-Bedrohungen entschärfen können. Leider wurde aufgrund von ungerechtfertigterweise wahrgenommenen rechtlichen Hürden kaum ein Opfer benachrichtigt oder unterstützt. Deshalb ist es wichtig, dass die NIS2 eine klare Rechtsgrundlage schafft, damit solche Bedrohungen entschärft und Informationen nicht nur innerhalb der EU, sondern auch mit Partnern außerhalb der EU ausgetauscht werden können.

Mit der Erweiterung des Aufgabenbereichs müssen sich CSIRT darauf vorbereiten, **skalierbare und automatisierte Lösungen** für die schnelle und sichere Verteilung von koordinierten Schwachstellenmeldungen, Sicherheitsvorfalls berichten und Bedrohungsinformationen anzubieten. Die Automatisierung des Informationsaustauschs ist nicht nur ein Derivat dieser Richtlinie; sie ist ihr Kernstück. Die Schaffung einer **rechtlichen Grundlage für CSIRT und Unternehmen, damit sie Daten** mit ihren Kunden, Kollegen und Behörden sowohl innerhalb als auch außerhalb der EU **austauschen** können, ist eine Voraussetzung für die Verwirklichung aller guten Absichten der NIS2.

Ein weiterer positiver Aspekt des Kommissionsvorschlags ist die Verwendung von **Normen und Zertifizierungssystemen**. Die Zertifizierung sollte durch spezielle europäische und international anerkannte Systeme, die nationalen Systemen vorzuziehen sind, möglich sein. Das Ziel sollte die Harmonisierung sein. Es sollten ähnliche Regeln in allen Mitgliedstaaten

gelten.

Der NIS2-Vorschlag sieht vor, dass die ENISA ein europäisches Schwachstellenregister entwickelt und pflegt. Der Berichterstatter ist der Ansicht, dass eine **europäische Datenbank für Schwachstellen** einem Register vorzuziehen ist. Es macht wenig Sinn, das zu verdoppeln, was bereits vorhanden ist und von der Cybersicherheits-Community als gemeinsamer Standard in allen Teilen der Welt verwendet wird. Eine Verdoppelung führt zu Zwietracht und Verwirrung innerhalb der Expertengemeinschaft. Eine europäische Datenbank, nicht ein Register, sollte das CVE-Register nutzen: die Liste der Aufzeichnungen über internationale, öffentlich bekannte Cybersicherheitsschwachstellen, die auf der ganzen Welt verwendet werden. Der Berichterstatter ist der Ansicht, dass ENISA eine herausragende neue Rolle innerhalb des CVE-Registers einnehmen sollte, das jetzt hauptsächlich in den USA angesiedelt ist. Darüber hinaus sollte Doppelarbeit vermieden werden; das wünschenswerte Ergebnis sollte eine Datenbank mit einzigartigen Herausforderungen für europäische Organisationen sein. Abschließend, aber dennoch wichtig: Der Berichterstatter betont, dass es für die ENISA von größter Bedeutung ist, über die Infrastruktur und die Verfahren für den Umgang mit Verschlusssachen zu verfügen. Die Cybersicherheit sollte von der Geheimhaltungsstufe bis zur (streng) geheimen Stufe behandelt werden.

WHOIS-Daten, die maßgebliche Aufzeichnung der Domain-Besitzverhältnisse, sind das einzige brauchbare Mittel, um die Informationen zu erhalten, die notwendig sind, um kriminelle Akteure zu identifizieren, Bedrohungsakteure aufzuspüren, Schäden zu verhindern und das Online-Ökosystem zu schützen. Die Cybersicherheits-Community verlässt sich darauf, und es ermöglicht Bedrohungsforschern, Gegner zu jagen, so dass sich Bürger und Unternehmen vor kommenden Bedrohungen schützen können. Es ist der einzige verlässliche Rechenschaftsmechanismus in einem ansonsten anonymen Internet. In den letzten drei Jahren, nach dem Inkrafttreten der DSGVO, werden WHOIS-Daten jedoch von einigen als ein Haftungsthema angesehen. Die gängige Nutzung der WHOIS-Daten wurde leider und unberechtigterweise gestoppt. Der Berichterstatter bekräftigt daher in seinem Bericht die Rechtmäßigkeit der Verarbeitung von Daten aus Gründen der Cybersicherheit im Rahmen der DSGVO mit dem ausdrücklichen legislativen Wunsch nach einem erneuten Austausch von WHOIS-Daten.

Insgesamt ist der Berichterstatter der Ansicht, dass die NIS2 der notwendige Schritt ist, um unseren Binnenmarkt zu harmonisieren und die Cybersicherheit in der gesamten EU zu verbessern.

15.10.2021

STELLUNGNAHME DES AUSSCHUSSES FÜR BÜRGERLICHE FREIHEITEN, JUSTIZ UND INNERES

für den Ausschuss für Industrie, Forschung und Energie

zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Verfasser der Stellungnahme (*): Lukas Mandl

(*) Assoziierter Ausschuss – Artikel 57 der Geschäftsordnung

KURZE BEGRÜNDUNG

Der Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)[1] ist Teil eines umfassenderen Pakets von Initiativen auf Ebene der Union, mit denen die Widerstandsfähigkeit öffentlicher und privater Einrichtungen gegenüber Bedrohungen erhöht werden soll. Mit dem Vorschlag sollen die Lücken in den bestehenden Rechtsvorschriften angegangen und die in ihren Anwendungsbereich fallenden Einrichtungen in die Lage versetzt werden, besser auf die neuen Herausforderungen zu reagieren, die von der Kommission in ihrer Folgenabschätzung, die auch eine umfassende Konsultation von Interessenträgern beinhaltete, ermittelt wurden. Zu diesen Herausforderungen gehören die zunehmende Digitalisierung des Binnenmarkts und die sich entwickelnde Sicherheitsbedrohungslage.

Die Rechtsgrundlage des Vorschlags bildet Artikel 114 AEUV, d. h der Binnenmarkt. Aus Sicht des LIBE-Ausschusses ist es jedoch wichtig, hervorzuheben, dass die Maßnahmen, die Netz- und Informationssystemen mit der NIS-2-Richtlinie auferlegt wurden, nicht nur dazu dienen, das ordnungsgemäße Funktionieren des Binnenmarkts sicherzustellen. **Die Richtlinie sollte auch zur Sicherheit der gesamten Union beitragen**, unter anderem indem eine unterschiedliche Anfälligkeit der Mitgliedstaaten gegenüber Cybersicherheitsrisiken verhindert wird.

Zu diesem Zweck ist es von entscheidender Bedeutung, **bestehende Unterschiede zwischen**

[1] 2020/0359(COD).

den Mitgliedstaaten, die sich aus verschiedenen Auslegungen der Rechtsvorschriften durch die Mitgliedstaaten ergeben, **zu beseitigen**. Daher begrüßt der Verfasser der Stellungnahme die mit der Verordnung festgelegte einheitliche Bedingung, mit der bestimmt wird, welche Einrichtungen in den Anwendungsbereich der Richtlinie fallen. Um Unterschiede bei der Umsetzung zu verhindern, werden zusätzliche Vorschläge unterbreitet, wobei insbesondere vorgesehen ist, dass die Kommission verpflichtet wird, Leitlinien zur Umsetzung der lex specialis und zu den für KMU geltenden Kriterien herauszugeben (die Rechtssicherheit bieten und unnötigen Aufwand verhindern sollten) und dass die Kooperationsgruppe verpflichtet wird, die nichttechnischen Faktoren, die bei den Lieferketten-Risikobewertungen zu berücksichtigen sind, näher zu bestimmen. Darüber hinaus wird betont, dass die Zusammenarbeit zwischen den zuständigen Behörden, sowohl innerhalb der Mitgliedstaaten als auch *zwischen* den Mitgliedstaaten in Echtzeit stattfinden muss.

Der Entwurf eines Berichts trägt auch einer Reihe von **Empfehlungen des EDSB** Rechnung, die in dessen Stellungnahme zur Cybersicherheitsstrategie und zur NIS-2-Richtlinie[2] unterbreitet wurden. Insbesondere wird sowohl in den Erwägungsgründen als auch im verfügenden Teil des Textes deutlich gemacht, dass die Verarbeitung personenbezogener Daten gemäß der NIS-2-Richtlinie nicht die Verordnung (EU) 2016/679 (DSGVO)[3] und die Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation)[4] berührt. Da der Begriff „Sicherheit von Netz- und Informationssystemen“ (der nur den Schutz von Technologien abdeckt) enger gefasst ist als der Begriff „Cybersicherheit“ (der auch Tätigkeiten zum Schutz von Nutzern abdeckt), wird der erstgenannte Begriff nur im rein technischen Kontext verwendet. Im Zusammenhang mit Domänennamen und Registrierungsdaten werden Präzisierungen vorgeschlagen, die folgende Aspekte betreffen: die Rechtsgrundlage für die Veröffentlichung „einschlägiger Angaben“ zu Zwecken der Identifizierung und Kontaktaufnahme, 2) die Kategorien von Daten über die Registrierung der Domänennamen, die einer Veröffentlichung unterliegen (beruhend auf einer Empfehlung der Zentralstelle für die Vergabe von Internet-Namen und -Adressen (ICANN)) und 3) die Einrichtungen, die „berechtigte Zugangsnachfrager“ darstellen könnten. In dem Rechtstext wird ferner präzisiert, dass der Vorschlag nicht die Zuweisung von Zuständigkeiten und Befugnissen von Datenschutzaufsichtsbehörden gemäß der DSGVO berührt. Schließlich wird eine umfassendere Rechtsgrundlage für die Zusammenarbeit und den Austausch einschlägiger Informationen zwischen den zuständigen Behörden gemäß dem Vorschlag und sonstigen Aufsichtsbehörden, insbesondere Aufsichtsbehörden gemäß der DSGVO, geschaffen.

Weitere Änderungen, die vom Verfasser der Stellungnahme des LIBE-Ausschusses am Vorschlag der Kommission vorgenommen wurden, betreffen die folgenden Aspekte:

- Um für Kohärenz zwischen der NIS-2-Richtlinie und der vorgeschlagenen Richtlinie

[2] Stellungnahme Nr. 5/2021: https://edps.europa.eu/system/files/2021-05/21-03-11_edps_nis2-opinion_de_0.pdf

[3] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), ABl. L 119 vom 4.5.2016, S. 1.

[4] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.7.2002, S. 37.

über die Resilienz kritischer Einrichtungen[5] zu sorgen, wurde der Wortlaut einiger Bestimmungen an den des letztgenannten Vorschlags angeglichen. Im Einklang mit einer ähnlichen Änderung, die für die Richtlinie über die Resilienz kritischer Einrichtungen vorgesehen ist, die die gleichen Sektoren abdecken sollte wie die NIS-2-Richtlinie, wird vorgeschlagen, „Herstellung, Verarbeitung und Vertrieb von Lebensmitteln“ zum Anwendungsbereich hinzuzufügen.

- In Bezug auf personenbezogene Daten wird klargestellt, dass die Überprüfung von Netz- und Informationssystemen durch CSIRTs nicht nur mit der Verordnung (EU) 2016/679 (DSGVO)[6], sondern auch mit der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation)[7] im Einklang stehen sollte. Internationale Übermittlungen personenbezogener Daten gemäß dieser Richtlinie sollten mit Kapitel V der DSGVO im Einklang stehen.
- Die Kooperationsgruppe sollte zweimal statt einmal jährlich zusammentreten, um eine Bestandsaufnahme der jüngsten Entwicklungen im Bereich der Cybersicherheit vorzunehmen. Der EDSA sollte als Beobachter an den Sitzungen der Kooperationsgruppe teilnehmen.
- Die ENISA sollte jährlich statt alle zwei Jahre Berichte über den Stand der Cybersicherheit in der Union veröffentlichen. Der Bericht sollte auch den Auswirkungen von Cybersicherheitsvorfällen auf den Schutz personenbezogener Daten in der Union Rechnung tragen.
- Die Frist für die Meldung von Vorfällen wird an die Frist für die Meldung von Verstößen gemäß der DSGVO angepasst, die 72 Stunden beträgt.
- Die Meldung tatsächlicher Cybersicherheitsvorfälle durch wesentliche und wichtige Einrichtungen sollte in der Tat verpflichtend sein, die Meldung von Cyberbedrohungen hingegen sollte freiwillig sein, um den Verwaltungsaufwand zu verringern und ausufernde Meldungen zu verhindern. Um als erheblich zu gelten, sollte ein Vorfall tatsächlich einen Schaden verursacht und sich auf andere natürliche und juristische Personen ausgewirkt haben, statt einen derartigen Schaden oder eine derartige Wirkung nur ermöglicht zu haben.
- Die Umstände, die bei der Entscheidung über Sanktionen infolge eines Verstoßes gegen die Cybersicherheitsvorschriften zu berücksichtigen sind, werden an die DSGVO angepasst. Es sollte nicht möglich sein, natürlichen Personen die Ausübung von Leitungsaufgaben vorübergehend zu untersagen, da dies den derzeitigen Haftungsregelungen des Unionsrechts zuwiderlaufen würde.
- Um Rufschädigung zu vermeiden, sollten Einrichtungen nicht verpflichtet werden, Aspekte der Nichteinhaltung der in dieser Richtlinie festgelegten Verpflichtungen oder die Identität der für den Verstoß verantwortlichen natürlichen oder juristischen Personen öffentlich bekannt zu machen.

---

[5] 2020/0365(COD).

[6] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), ABl. L 119 vom 4.5.2016, S. 1.

[7] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.7.2002, S. 37.

ÄNDERUNGSANTRÄGE

Der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres ersucht den federführenden Ausschuss für Industrie, Forschung und Energie, folgende Änderungsanträge zu berücksichtigen:

Änderungsantrag 1

Vorschlag für eine Richtlinie
Erwägung 1

Vorschlag der Kommission	*Geänderter Text*
(1) Ziel der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates[11] war der unionsweite Aufbau von Cybersicherheitskapazitäten, die Eindämmung von Bedrohungen für Netz- und Informationssysteme, die zur Erbringung wesentlicher Dienste in Schlüsselsektoren verwendet werden, und die Sicherstellung der Kontinuität solcher Dienste bei Cybersicherheitsvorfällen, um so zum reibungslosen Funktionieren ***der*** Wirtschaft und Gesellschaft ***der Union*** beizutragen.	(1) Ziel der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates[11] war der unionsweite Aufbau von Cybersicherheitskapazitäten, die Eindämmung von Bedrohungen für Netz- und Informationssysteme, die zur Erbringung wesentlicher Dienste in Schlüsselsektoren verwendet werden, und die Sicherstellung der Kontinuität solcher Dienste bei Cybersicherheitsvorfällen, um so ***zur Sicherheit der Union und*** zum reibungslosen Funktionieren ***ihrer*** Wirtschaft und Gesellschaft beizutragen.
[11] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).	[11] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

Änderungsantrag 2

Vorschlag für eine Richtlinie
Erwägung 2

Vorschlag der Kommission	*Geänderter Text*
(2) Seit Inkrafttreten der Richtlinie (EU) 2016/1148 sind erhebliche Fortschritte bei der Stärkung der Cyberresilienz der Union erzielt worden. Die Überprüfung jener Richtlinie hat	(2) Seit Inkrafttreten der Richtlinie (EU) 2016/1148 sind erhebliche Fortschritte bei der Stärkung der Cyberresilienz der Union erzielt worden. Die Überprüfung jener Richtlinie hat

gezeigt, dass sie als Katalysator für das institutionelle und regulatorische Cybersicherheitskonzept in der Union gedient und ein erhebliches Umdenken bewirkt hat. Durch die Festlegung nationaler Cybersicherheitsstrategien, die Schaffung nationaler Kapazitäten und die Umsetzung von Regulierungsmaßnahmen für Infrastrukturen und Akteure, die von den einzelnen Mitgliedstaaten als wesentlich eingestuft wurden, wurde mit jener Richtlinie die Vervollständigung der nationalen Rechtsrahmen sichergestellt. Darüber hinaus hat sie durch die Einrichtung der Kooperationsgruppe[12] und eines Netzwerks nationaler Reaktionsteams für IT-Sicherheitsvorfälle (CSIRT-Netzwerk)[13] zur Zusammenarbeit auf Unionsebene beigetragen. Ungeachtet dieser Erfolge hat die Überprüfung der Richtlinie (EU) 2016/1148 inhärente Mängel ergeben, die ein wirksames Vorgehen gegen aktuelle und neue Herausforderungen im Bereich Cybersicherheit verhindern.

[12] Artikel 11 der Richtlinie (EU) 2016/1148.

[13] Artikel 12 der Richtlinie (EU) 2016/1148.

gezeigt, dass sie als Katalysator für das institutionelle und regulatorische Cybersicherheitskonzept in der Union gedient und ein erhebliches Umdenken bewirkt hat. Durch die Festlegung nationaler Cybersicherheitsstrategien, die Schaffung nationaler Kapazitäten und die Umsetzung von Regulierungsmaßnahmen für Infrastrukturen und Akteure, die von den einzelnen Mitgliedstaaten als wesentlich eingestuft wurden, wurde mit jener Richtlinie die Vervollständigung der nationalen Rechtsrahmen sichergestellt. Darüber hinaus hat sie durch die Einrichtung der Kooperationsgruppe und eines Netzwerks nationaler Reaktionsteams für IT-Sicherheitsvorfälle (CSIRT-Netzwerk) zur Zusammenarbeit auf Unionsebene beigetragen. Ungeachtet dieser Erfolge hat die Überprüfung der Richtlinie (EU) 2016/1148 inhärente Mängel ergeben, die ein wirksames Vorgehen gegen aktuelle und neue Herausforderungen im Bereich Cybersicherheit verhindern. ***Darüber hinaus wurde durch die Ausweitung der Online-Tätigkeiten im Rahmen der COVID-19-Pandemie die Bedeutung von Cybersicherheit, die unerlässlich ist, damit die EU-Bürger in Innovation und Konnektivität vertrauen können, und von umfassender Aus- und Weiterbildung in diesem Bereich deutlich. Die Kommission sollte die Mitgliedstaaten daher bei der Konzeption von Bildungsprogrammen zur Cybersicherheit unterstützen, um wichtige und wesentliche Einrichtungen in die Lage zu versetzen, Sachverständige für Cybersicherheit einzustellen, die es ihnen ermöglichen, den sich aus dieser Richtlinie ergebenden Verpflichtungen nachzukommen.***

[12] Artikel 11 der Richtlinie (EU) 2016/1148.

[13] Artikel 12 der Richtlinie (EU) 2016/1148.

Änderungsantrag 3

Vorschlag für eine Richtlinie
Erwägung 3

Vorschlag der Kommission	*Geänderter Text*
(3) Netz- und Informationssysteme sind durch den schnellen digitalen Wandel und die Vernetzung der Gesellschaft zu einem zentralen Bestandteil des Alltags und für den grenzüberschreitenden Austausch geworden. Diese Entwicklung hat zu einer Ausweitung der Bedrohungslage im Bereich der Cybersicherheit geführt und neue Herausforderungen mit sich gebracht, die in allen Mitgliedstaaten entsprechende koordinierte und innovative Reaktionen erfordern. Die Anzahl, Tragweite, Komplexität, Häufigkeit und Auswirkungen von Cybersicherheitsvorfällen nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen dar. Im Ergebnis können Cybersicherheitsvorfälle die Ausübung wirtschaftlicher Tätigkeiten im Binnenmarkt beeinträchtigen, finanzielle Verluste verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft und Gesellschaft ***der Union*** großen Schaden zufügen. ***Heute sind daher im Bereich Cybersicherheit*** Vorsorge und Wirksamkeit wichtiger denn je für das reibungslose Funktionieren des Binnenmarkts.	(3) Netz- und Informationssysteme sind durch den schnellen digitalen Wandel und die Vernetzung der Gesellschaft zu einem zentralen Bestandteil des Alltags und für den grenzüberschreitenden Austausch geworden. Diese Entwicklung hat zu einer Ausweitung der Bedrohungslage im Bereich der Cybersicherheit geführt und neue Herausforderungen mit sich gebracht, die in allen Mitgliedstaaten entsprechende koordinierte und innovative Reaktionen erfordern. Die Anzahl, Tragweite, Komplexität, Häufigkeit und Auswirkungen von Cybersicherheitsvorfällen nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen dar. Im Ergebnis können Cybersicherheitsvorfälle die Ausübung wirtschaftlicher Tätigkeiten im Binnenmarkt beeinträchtigen, finanzielle Verluste verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft ***der Union, der Funktionsfähigkeit unserer Demokratie*** und ***den Werten und Freiheiten, auf denen unsere*** Gesellschaft ***beruht,*** großen Schaden zufügen. ***Vor dem Hintergrund des digitalen Wandels der täglichen Tätigkeiten in der gesamten Union sind daher*** Vorsorge und Wirksamkeit ***im Bereich Cybersicherheit heute*** wichtiger denn je für ***die Sicherheit in der Union und*** das reibungslose Funktionieren des Binnenmarkts. ***Dies erfordert eine engere Zusammenarbeit in und zwischen den Mitgliedstaaten sowie zwischen nationalen Behörden und den zuständigen Stellen der Union.***

Änderungsantrag 4

Vorschlag für eine Richtlinie
Erwägung 5

Vorschlag der Kommission	*Geänderter Text*
(5) All diese Unterschiede führen zu einer Fragmentierung des Binnenmarkts und können sich nachteilig auf dessen Funktionieren auswirken und aufgrund der Anwendung unterschiedlicher Normen insbesondere die grenzüberschreitende Erbringung von Diensten und das Niveau der Cyberresilienz beeinträchtigen. Ziel der vorliegenden Richtlinie ist, diese großen Unterschiede zwischen den Mitgliedstaaten zu beseitigen, indem insbesondere Mindestvorschriften für einen funktionierenden und koordinierten Rechtsrahmen festgelegt werden, Mechanismen für die wirksame Zusammenarbeit zwischen den zuständigen Behörden in den einzelnen Mitgliedstaaten vorgesehen werden, die Liste der Sektoren und Tätigkeiten, die Pflichten im Hinblick auf die Cybersicherheit unterliegen, aktualisiert wird und wirksame Abhilfemaßnahmen und Sanktionen, die für die wirksame Durchsetzung dieser Verpflichtungen von entscheidender Bedeutung sind, eingeführt werden. Daher sollte die Richtlinie (EU) 2016/1148 aufgehoben und durch die vorliegende Richtlinie ersetzt werden.	(5) All diese Unterschiede führen zu einer Fragmentierung des Binnenmarkts und können sich nachteilig auf dessen Funktionieren auswirken und aufgrund der Anwendung unterschiedlicher Normen insbesondere die grenzüberschreitende Erbringung von Diensten und das Niveau der Cyberresilienz beeinträchtigen. ***Letztendlich können diese Unterschiede zu einer höheren Anfälligkeit einiger Mitgliedstaaten gegenüber Cybersicherheitsbedrohungen führen, deren Auswirkungen auf die gesamte Union übergreifen könnten, sowohl im Hinblick auf ihren Binnenmarkt, als auch im Hinblick auf die allgemeine Sicherheit.*** Ziel der vorliegenden Richtlinie ist, diese großen Unterschiede zwischen den Mitgliedstaaten zu beseitigen, indem insbesondere Mindestvorschriften für einen funktionierenden und koordinierten Rechtsrahmen festgelegt werden, Mechanismen für die wirksame Zusammenarbeit ***in Echtzeit*** zwischen den zuständigen Behörden in den einzelnen Mitgliedstaaten ***und zwischen den zuständigen Behörden der Mitgliedstaaten*** vorgesehen werden, die Liste der Sektoren und Tätigkeiten, die Pflichten im Hinblick auf die Cybersicherheit unterliegen, aktualisiert wird und wirksame Abhilfemaßnahmen und Sanktionen, die für die wirksame Durchsetzung dieser Verpflichtungen von entscheidender Bedeutung sind, eingeführt werden. Daher sollte die Richtlinie (EU) 2016/1148 aufgehoben und durch die vorliegende Richtlinie ersetzt werden.

Änderungsantrag 5

Vorschlag für eine Richtlinie
Erwägung 6

Vorschlag der Kommission	*Geänderter Text*
(6) Im Einklang mit dem Unionsrecht bleibt die Möglichkeit der Mitgliedstaaten, die für die Wahrung ihrer wesentlichen Sicherheitsinteressen und den Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit erforderlichen Maßnahmen zu ergreifen und die Ermittlung, Feststellung und Verfolgung von Straftaten zuzulassen, von der vorliegenden Richtlinie unberührt. Nach Artikel 346 AEUV ist kein Mitgliedstaat verpflichtet, Auskünfte zu erteilen, deren Preisgabe seinen wesentlichen Sicherheitsinteressen widerspräche. In diesem Zusammenhang sind nationale und Unionsvorschriften zum Schutz von Verschlusssachen, Geheimhaltungsvereinbarungen und informelle Geheimhaltungsvereinbarungen wie das sogenannte Traffic Light Protocol[14] von Bedeutung.	(6) Im Einklang mit dem Unionsrecht bleibt die Möglichkeit der Mitgliedstaaten, die für die Wahrung ihrer wesentlichen ***nationalen*** Sicherheitsinteressen und den Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit erforderlichen Maßnahmen zu ergreifen und die ***Verhütung,*** Ermittlung, Feststellung und Verfolgung von Straftaten zuzulassen, von der vorliegenden Richtlinie unberührt. Nach Artikel 346 AEUV ist kein Mitgliedstaat verpflichtet, Auskünfte zu erteilen, deren Preisgabe seinen wesentlichen Sicherheitsinteressen widerspräche. In diesem Zusammenhang sind nationale und Unionsvorschriften zum Schutz von Verschlusssachen, Geheimhaltungsvereinbarungen und informelle Geheimhaltungsvereinbarungen wie das sogenannte Traffic Light Protocol[14] von Bedeutung.
[14] Mithilfe des Traffic Light Protocol (TLP) kann jemand, der Informationen weitergibt, die Empfänger über etwaige Einschränkungen bei der weiteren Verbreitung dieser Informationen informieren. Es wird in fast allen CSIRT-Gemeinschaften und einigen Informationsaustausch- und -analysezentren (Information Sharing and Analysis Centres – ISACs) genutzt.	[14] Mithilfe des Traffic Light Protocol (TLP) kann jemand, der Informationen weitergibt, die Empfänger über etwaige Einschränkungen bei der weiteren Verbreitung dieser Informationen informieren. Es wird in fast allen CSIRT-Gemeinschaften und einigen Informationsaustausch- und -analysezentren (Information Sharing and Analysis Centres – ISACs) genutzt.

Änderungsantrag 6

Vorschlag für eine Richtlinie
Erwägung 8

Vorschlag der Kommission	*Geänderter Text*
(8) ***Gemäß*** der Richtlinie (EU) 2016/1148 ***waren die Mitgliedstaaten dafür zuständig zu bestimmen***, welche Einrichtungen die Kriterien für die Einstufung als Betreiber wesentlicher Dienste erfüllen („Ermittlungsprozess“)***.*** ***Um die diesbezüglichen*** großen ***Unterschiede*** zwischen den Mitgliedstaaten ***zu beheben und für alle relevanten Einrichtungen Rechtssicherheit hinsichtlich*** der ***Risikomanagementanforderungen und der Meldepflichten zu gewährleisten***, sollte ein einheitliches Kriterium dafür festgelegt werden, welche Einrichtungen in den Anwendungsbereich der vorliegenden Richtlinie fallen. Dieses Kriterium sollte in der Anwendung des Schwellenwerts für die Größe bestehen, nach der alle mittleren und großen Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission[15]***,*** die in den Sektoren tätig sind oder die Art von Diensten erbringen, die unter die vorliegende Richtlinie fallen, in den Anwendungsbereich der Richtlinie fallen. Die Mitgliedstaaten sollten nicht verpflichtet sein, eine Liste der Einrichtungen zu erstellen, die dieses allgemein anwendbare größenbezogene Kriterium erfüllen.	(8) ***Die Zuständigkeit der Mitgliedstaaten, die gemäß*** der Richtlinie (EU)2016/1148 ***bestimmen mussten***, welche Einrichtungen die Kriterien für die Einstufung als Betreiber wesentlicher Dienste erfüllen („Ermittlungsprozess“)***, hat diesbezüglich zu*** großen ***Unterschieden*** zwischen den Mitgliedstaaten ***geführt. Unbeschadet*** der ***in dieser Richtlinie vorgesehenen spezifischen Ausnahmen***, sollte ein einheitliches Kriterium dafür festgelegt werden, welche Einrichtungen in den Anwendungsbereich der vorliegenden Richtlinie fallen***, um diese Unterschiede zu beseitigen und hinsichtlich der Risikomanagementanforderungen und der Meldepflichten für alle einschlägigen Einrichtungen für Rechtssicherheit zu sorgen***. Dieses Kriterium sollte in der Anwendung des Schwellenwerts für die Größe bestehen, nach der alle mittleren und großen Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission[15], die in den Sektoren tätig sind oder die Art von Diensten erbringen, die unter die vorliegende Richtlinie fallen, in den Anwendungsbereich der Richtlinie fallen. Die Mitgliedstaaten sollten nicht verpflichtet sein, eine Liste der Einrichtungen zu erstellen, die dieses allgemein anwendbare größenbezogene Kriterium erfüllen.
[15] Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).	[15] Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).

Änderungsantrag 7

Vorschlag für eine Richtlinie
Erwägung 8 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(8a) Angesichts der Unterschiede bei den nationalen Rahmen für die öffentliche Verwaltung behalten die Mitgliedstaaten ihre Entscheidungsbefugnis in Bezug auf die Benennung von Einrichtungen im Rahmen des Anwendungsbereichs der vorliegenden Richtlinie.

Änderungsantrag 8

Vorschlag für eine Richtlinie
Erwägung 9

Vorschlag der Kommission	*Geänderter Text*
(9) ***Allerdings sollten auch*** Klein- und Kleinsteinrichtungen, die bestimmte Kriterien erfüllen, nach denen sie eine Schlüsselrolle für die Wirtschaft oder Gesellschaft des betreffenden Mitgliedstaats oder für bestimmte Sektoren oder Arten von Diensten spielen, von der vorliegenden Richtlinie erfasst werden. Die Mitgliedstaaten sollten für die Erstellung einer Liste solcher Einrichtungen zuständig sein und diese der Kommission übermitteln.	(9) ***Auch*** Klein- und Kleinsteinrichtungen, die bestimmte Kriterien erfüllen, nach denen sie ***auf der Grundlage einer Risikobewertung*** eine Schlüsselrolle für die Wirtschaft oder Gesellschaft des betreffenden Mitgliedstaats oder für bestimmte Sektoren oder Arten von Diensten spielen, ***einschließlich Einrichtungen, die gemäß der Richtlinie (EU) XXX/XXX des Europäischen Parlaments und des Rates[1a] als kritische Einrichtungen oder als kritischen Einrichtungen gleichwertige Einrichtungen definiert sind, sollten*** von der vorliegenden Richtlinie erfasst werden. Die Mitgliedstaaten sollten für die Erstellung einer Liste solcher Einrichtungen zuständig sein und diese der Kommission übermitteln.
	_____
	1aRichtlinie (EU) [XXX/XXX] des Europäischen Parlaments und des Rates vom XXX über die Resilienz kritischer Einrichtungen (ABl. ...).

Änderungsantrag 9

Vorschlag für eine Richtlinie
Erwägung 10

Vorschlag der Kommission	*Geänderter Text*
(10) Die Kommission ***kann*** in Zusammenarbeit mit der Kooperationsgruppe Leitlinien für die Anwendung der für Klein- und ***Kleinstunternehmen*** geltenden Kriterien herausgeben.	(10) Die Kommission ***sollte*** in Zusammenarbeit mit der Kooperationsgruppe Leitlinien für die Anwendung der für Klein- und ***Kleinsteinrichtungen*** geltenden Kriterien herausgeben.

Änderungsantrag 10

Vorschlag für eine Richtlinie
Erwägung 12

Vorschlag der Kommission	*Geänderter Text*
(12) Durch sektorspezifische Rechtsvorschriften und Instrumente kann dazu beigetragen werden, ein hohes Maß an Cybersicherheit zu gewährleisten und gleichzeitig den Besonderheiten und Komplexitäten der Sektoren in vollem Umfang Rechnung zu tragen. Müssen wesentliche oder wichtige Einrichtungen gemäß einem sektorspezifischen Rechtsakt der Union Maßnahmen zum Cybersicherheitsrisikomanagement ergreifen oder Sicherheitsvorfälle oder erhebliche Cyberbedrohungen melden und ist dies in der Wirkung den in der vorliegenden Richtlinie festgelegten Verpflichtungen mindestens gleichwertig, so sollten diese sektorspezifischen Bestimmungen, einschließlich in Bezug auf Aufsicht und Durchsetzung, Anwendung finden. Die Kommission ***kann*** Leitlinien im Zusammenhang mit der Umsetzung der lex specialis herausgeben. Die vorliegende Richtlinie schließt nicht aus, dass zusätzliche sektorspezifische Rechtsakte der Union zu Maßnahmen zum Cybersicherheitsrisikomanagement und zur Meldung von Sicherheitsvorfällen erlassen	(12) Durch sektorspezifische Rechtsvorschriften und Instrumente kann dazu beigetragen werden, ein hohes Maß an Cybersicherheit zu gewährleisten und gleichzeitig den Besonderheiten und Komplexitäten der Sektoren in vollem Umfang Rechnung zu tragen. Müssen wesentliche oder wichtige Einrichtungen gemäß einem sektorspezifischen Rechtsakt der Union Maßnahmen zum Cybersicherheitsrisikomanagement ergreifen oder Sicherheitsvorfälle oder erhebliche Cyberbedrohungen melden und ist dies in der Wirkung den in der vorliegenden Richtlinie festgelegten Verpflichtungen mindestens gleichwertig, so sollten diese sektorspezifischen Bestimmungen, einschließlich in Bezug auf Aufsicht und Durchsetzung, Anwendung finden. Die Kommission ***sollte*** Leitlinien im Zusammenhang mit der Umsetzung der lex specialis herausgeben. Die vorliegende Richtlinie schließt nicht aus, dass zusätzliche sektorspezifische Rechtsakte der Union zu Maßnahmen zum Cybersicherheitsrisikomanagement und zur Meldung von Sicherheitsvorfällen erlassen

werden. Die vorliegende Richtlinie berührt nicht die bestehenden Durchführungsbefugnisse, die der Kommission in einer Reihe von Sektoren, darunter Verkehr und Energie, übertragen wurden.

werden. Die vorliegende Richtlinie berührt nicht die bestehenden Durchführungsbefugnisse, die der Kommission in einer Reihe von Sektoren, darunter Verkehr und Energie, übertragen wurden.

Änderungsantrag 11

Vorschlag für eine Richtlinie
Erwägung 14

Vorschlag der Kommission	*Geänderter Text*
(14) Angesichts der Zusammenhänge zwischen der Cybersicherheit und der physischen Sicherheit von Einrichtungen sollte dafür gesorgt werden, dass der Ansatz der Richtlinie (EU) XXX/XXX des Europäischen Parlaments und des Rates[17] und der Ansatz der vorliegenden Richtlinie kohärent sind. Um dies zu erreichen, sollten die Mitgliedstaaten sicherstellen, dass kritische Einrichtungen und diesen gleichgestellte Einrichtungen im Sinne der Richtlinie (EU) XXX/XXX als wesentliche Einrichtungen im Sinne der vorliegenden Richtlinie gelten. Die Mitgliedstaaten sollten auch sicherstellen, dass ihre Cybersicherheitsstrategien einen politischen Rahmen für eine verstärkte Koordinierung zwischen ***der*** gemäß der vorliegenden Richtlinie zuständigen ***Behörde*** und der gemäß Richtlinie (EU) XXX/XXX zuständigen Behörde beim Informationsaustausch über ***Sicherheitsvorfälle*** und Cyberbedrohungen und bei der Wahrnehmung von Aufsichtsaufgaben vorsehen. Die gemäß diesen beiden Richtlinien zuständigen Behörden sollten zusammenarbeiten und Informationen austauschen, insbesondere in Bezug auf die Ermittlung kritischer Einrichtungen, Cyberbedrohungen, Cybersicherheitsrisiken und Sicherheitsvorfälle, die kritische Einrichtungen beeinträchtigen, sowie über die von ***kritischen Einrichtungen***	(14) Angesichts der Zusammenhänge zwischen der Cybersicherheit und der physischen Sicherheit von Einrichtungen sollte***, sofern möglich und angebracht,*** dafür gesorgt werden, dass der Ansatz der Richtlinie (EU) XXX/XXX des Europäischen Parlaments und des Rates[17] und der Ansatz der vorliegenden Richtlinie kohärent sind. Um dies zu erreichen, sollten die Mitgliedstaaten sicherstellen, dass kritische Einrichtungen und diesen gleichgestellte Einrichtungen im Sinne der Richtlinie (EU) XXX/XXX als wesentliche Einrichtungen im Sinne der vorliegenden Richtlinie gelten. Die Mitgliedstaaten sollten auch sicherstellen, dass ihre Cybersicherheitsstrategien einen politischen Rahmen für eine verstärkte Koordinierung zwischen ***den*** gemäß der vorliegenden Richtlinie zuständigen ***Behörden in und zwischen den Mitgliedstaaten*** und der gemäß ***der*** Richtlinie (EU) XXX/XXX zuständigen Behörde beim Informationsaustausch über ***Cybersicherheitsvorfälle*** und Cyberbedrohungen und bei der Wahrnehmung von Aufsichtsaufgaben vorsehen. Die gemäß diesen beiden Richtlinien zuständigen Behörden sollten ***in und zwischen den Mitgliedstaaten*** zusammenarbeiten und Informationen austauschen, insbesondere in Bezug auf die Ermittlung kritischer Einrichtungen, Cyberbedrohungen,

ergriffenen Cybersicherheitsmaßnahmen. Auf Ersuchen der gemäß der Richtlinie (EU) XXX/XXX zuständigen Behörden sollte den gemäß der vorliegenden Richtlinie zuständigen Behörden gestattet werden, ***ihre Aufsichts- und Durchsetzungsbefugnisse gegenüber*** einer als kritisch eingestuften wesentlichen Einrichtung ***auszuüben***. Beide Behörden sollten zu diesem Zweck zusammenarbeiten und Informationen austauschen.

Cybersicherheitsrisiken und Sicherheitsvorfälle, die kritische Einrichtungen beeinträchtigen, sowie über die von ***den zuständigen Behörden gemäß dieser Richtlinie*** ergriffenen ***für kritische Einrichtungen relevanten*** Cybersicherheitsmaßnahmen. Auf Ersuchen der gemäß der Richtlinie (EU) XXX/XXX zuständigen Behörden sollte den gemäß der vorliegenden Richtlinie zuständigen Behörden gestattet werden, ***die Cybersicherheit*** einer als kritisch eingestuften wesentlichen Einrichtung ***zu bewerten***. Beide Behörden sollten zu diesem Zweck zusammenarbeiten und ***in Echtzeit*** Informationen austauschen.

[17] [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].

[17] [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].

Änderungsantrag 12

Vorschlag für eine Richtlinie
Erwägung 18

Vorschlag der Kommission

(18) Dienste, die von Anbietern von Rechenzentrumsdiensten angeboten werden, werden möglicherweise nicht immer in Form eines Cloud-Computing-Diensts erbracht. Dementsprechend sind Rechenzentren möglicherweise nicht immer Teil einer Cloud-Computing-Infrastruktur. Um allen Risiken für die ***Sicherheit von Netz- und Informationssystemen*** zu begegnen, sollte die vorliegende Richtlinie auch für Anbieter solcher Rechenzentrumsdienste gelten, bei denen es sich nicht um Cloud-Computing-Dienste handelt. Für die Zwecke der vorliegenden Richtlinie sollte der Begriff „Rechenzentrumsdienst“ Dienstleistungen umfassen, mit denen Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die

Geänderter Text

(18) Dienste, die von Anbietern von Rechenzentrumsdiensten angeboten werden, werden möglicherweise nicht immer in Form eines Cloud-Computing-Diensts erbracht. Dementsprechend sind Rechenzentren möglicherweise nicht immer Teil einer Cloud-Computing-Infrastruktur. Um allen Risiken für die ***Cybersicherheit*** zu begegnen, sollte die vorliegende Richtlinie auch für Anbieter solcher Rechenzentrumsdienste gelten, bei denen es sich nicht um Cloud-Computing-Dienste handelt. Für die Zwecke der vorliegenden Richtlinie sollte der Begriff „Rechenzentrumsdienst“ Dienstleistungen umfassen, mit denen Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von Informationstechnologie und

Verbindung und den Betrieb von Informationstechnologie und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden. Der Begriff „Rechenzentrumsdienst“ gilt nicht für interne Rechenzentren, die sich im Besitz der betreffenden Einrichtung befinden und von ihr für eigene Zwecke betrieben werden.

Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden. Der Begriff „Rechenzentrumsdienst“ gilt nicht für interne Rechenzentren, die sich im Besitz der betreffenden Einrichtung befinden und von ihr für eigene Zwecke betrieben werden.

Änderungsantrag 13

Vorschlag für eine Richtlinie
Erwägung 20

Vorschlag der Kommission	*Geänderter Text*
(20) Diese wachsenden gegenseitigen Abhängigkeiten sind das Ergebnis eines sich über immer mehr Grenzen hinweg erstreckenden und zunehmend interdependenten Dienstleistungsnetzes, das zentrale Infrastrukturen in der gesamten Union nutzt, und zwar in den Sektoren Energie, Verkehr, digitale Infrastruktur, Trinkwasser und Abwasser, Gesundheit, bestimmten Bereichen der öffentlichen Verwaltung sowie im Weltraumsektor, soweit es um die Erbringung bestimmter Dienste geht, die von Bodeninfrastrukturen abhängig sind, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden; damit sind Infrastrukturen ausgenommen, die sich im Eigentum der Union befinden oder von der Union oder in ihrem Namen im Rahmen ihrer Weltraumprogramme verwaltet oder betrieben werden. Wegen dieser gegenseitigen Abhängigkeiten kann jede Störung, auch wenn sie anfänglich auf eine Einrichtung oder einen Sektor beschränkt ist, zu breiteren Kaskadeneffekten führen, die	(20) Diese wachsenden gegenseitigen Abhängigkeiten sind das Ergebnis eines sich über immer mehr Grenzen hinweg erstreckenden und zunehmend interdependenten Dienstleistungsnetzes, das zentrale Infrastrukturen in der gesamten Union nutzt, und zwar in den Sektoren Energie, Verkehr, digitale Infrastruktur, Trinkwasser und Abwasser, ***Herstellung, Verarbeitung und Vertrieb von Lebensmitteln,*** Gesundheit, bestimmten Bereichen der öffentlichen Verwaltung sowie im Weltraumsektor, soweit es um die Erbringung bestimmter Dienste geht, die von Bodeninfrastrukturen abhängig sind, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden; damit sind Infrastrukturen ausgenommen, die sich im Eigentum der Union befinden oder von der Union oder in ihrem Namen im Rahmen ihrer Weltraumprogramme verwaltet oder betrieben werden. Wegen dieser gegenseitigen Abhängigkeiten kann jede Störung, auch wenn sie anfänglich auf eine Einrichtung oder einen Sektor beschränkt

weitreichende und lang anhaltende negative Auswirkungen auf die Erbringung von Dienstleistungen im gesamten Binnenmarkt haben können. Die COVID-19-Pandemie ***hat*** gezeigt, wie anfällig unsere zunehmend interdependenten Gesellschaften für Risiken mit geringer Eintrittswahrscheinlichkeit sind.	ist, zu breiteren Kaskadeneffekten führen, die weitreichende und lang anhaltende negative Auswirkungen auf die Erbringung von Dienstleistungen im gesamten Binnenmarkt haben können. Die ***verstärkten Angriffe auf Informationssysteme während der*** COVID-19-Pandemie ***haben*** gezeigt, wie anfällig unsere zunehmend interdependenten Gesellschaften für Risiken mit geringer Eintrittswahrscheinlichkeit sind. ***Daher sind weitere Investitionen in die Cybersicherheit erforderlich.***

Änderungsantrag 14

Vorschlag für eine Richtlinie
Erwägung 20 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(20a) Es ist von entscheidender Bedeutung, in allen kritischen und wichtigen Einrichtungen, einschließlich Einrichtungen der öffentlichen Verwaltung, das Bewusstsein für Cybersicherheit zu schärfen und die Cyberabwehrfähigkeit zu steigern.

Änderungsantrag 15

Vorschlag für eine Richtlinie
Erwägung 21

Vorschlag der Kommission	*Geänderter Text*
(21) Angesichts der unterschiedlichen nationalen Governancestrukturen und zwecks Beibehaltung von bereits bestehenden sektorbezogenen Vereinbarungen und Aufsichts- oder Regulierungsstellen der Union sollten die Mitgliedstaaten befugt sein, mehr als eine nationale Behörde zu benennen, die für die	(21) Angesichts der unterschiedlichen nationalen Governancestrukturen und zwecks Beibehaltung von bereits bestehenden sektorbezogenen Vereinbarungen und Aufsichts- oder Regulierungsstellen der Union sollten die Mitgliedstaaten befugt sein, mehr als eine nationale Behörde zu benennen, die für die

Erfüllung der Aufgaben im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen von wesentlichen und wichtigen Einrichtungen gemäß der vorliegenden Richtlinie zuständig sind. Die Mitgliedstaaten sollten diese Funktion einer bestehenden Behörde zuweisen dürfen.	Erfüllung der Aufgaben im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen von wesentlichen und wichtigen Einrichtungen gemäß der vorliegenden Richtlinie zuständig sind. Die Mitgliedstaaten sollten diese Funktion einer bestehenden Behörde zuweisen dürfen ***und sicherstellen, dass diese über angemessene Ressourcen verfügt, damit sie ihre Aufgaben wirksam und effizient erfüllen kann***.

Änderungsantrag 16

Vorschlag für eine Richtlinie
Erwägung 22

Vorschlag der Kommission	*Geänderter Text*
(22) Zur Erleichterung der grenzüberschreitenden Zusammenarbeit und Kommunikation zwischen Behörden und um die wirksame Umsetzung der vorliegenden Richtlinie zu ermöglichen, ist es notwendig, dass jeder Mitgliedstaat eine nationale zentrale Anlaufstelle benennt, die für die Koordinierung im Zusammenhang mit der ***Sicherheit von Netz-und Informationssystemen*** und für die grenzüberschreitende Zusammenarbeit auf Unionsebene zuständig ist.	(22) Zur Erleichterung der grenzüberschreitenden Zusammenarbeit und Kommunikation zwischen Behörden und um die wirksame Umsetzung der vorliegenden Richtlinie zu ermöglichen, ist es notwendig, dass jeder Mitgliedstaat eine nationale zentrale Anlaufstelle benennt, die für die Koordinierung im Zusammenhang mit der ***Cybersicherheit*** und für die grenzüberschreitende Zusammenarbeit auf Unionsebene zuständig ist.

Änderungsantrag 17

Vorschlag für eine Richtlinie
Erwägung 23

Vorschlag der Kommission	*Geänderter Text*
(23) Einrichtungen sollten den zuständigen Behörden oder den CSIRTs Sicherheitsvorfälle wirksam und effizient melden. Die zentralen Anlaufstellen sollten beauftragt werden, die Meldungen über Sicherheitsvorfälle an die zentralen Anlaufstellen ***anderer betroffener*** Mitgliedstaaten weiterzuleiten. Damit	(23) Einrichtungen sollten den zuständigen Behörden oder den CSIRTs Sicherheitsvorfälle wirksam und effizient melden. Die zentralen Anlaufstellen sollten beauftragt werden, die Meldungen über Sicherheitsvorfälle ***in Echtzeit*** an die zentralen Anlaufstellen ***aller anderen*** Mitgliedstaaten weiterzuleiten. Damit

sichergestellt ist, dass es pro Mitgliedstaat nur eine einzige behördliche Anlaufstelle gibt, sollten die zentralen Anlaufstellen auch relevante Informationen über Vorfälle, die Einrichtungen des Finanzsektors betreffen, von den gemäß der Verordnung XXXX/XXXX zuständigen Behörden entgegennehmen, die sie gegebenenfalls gemäß der vorliegenden Richtlinie an die zuständigen nationalen Behörden oder CSIRTs weiterleiten können sollten.

sichergestellt ist, dass es pro Mitgliedstaat nur eine einzige behördliche Anlaufstelle gibt, sollten die zentralen Anlaufstellen auch relevante Informationen über Vorfälle, die Einrichtungen des Finanzsektors betreffen, von den gemäß der Verordnung XXXX/XXXX zuständigen Behörden entgegennehmen, die sie gegebenenfalls gemäß der vorliegenden Richtlinie an die zuständigen nationalen Behörden oder CSIRTs weiterleiten können sollten.

Änderungsantrag 18

Vorschlag für eine Richtlinie
Erwägung 25

Vorschlag der Kommission	*Geänderter Text*
(25) In Bezug auf personenbezogene Daten sollten CSIRTs in der Lage sein, im Einklang mit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[19] im Namen und auf Ersuchen einer unter die vorliegende Richtlinie fallenden Einrichtung eine ***proaktive Überprüfung*** der für die Bereitstellung ihrer Dienste verwendeten ***Netz-*** und ***Informationssysteme auf Schwachstellen vorzunehmen***. Die Mitgliedstaaten sollten für alle sektorbezogenen CSIRTs ein vergleichbares Niveau an technischen Kapazitäten anstreben. Die Mitgliedstaaten können die Agentur der Europäischen Union für Cybersicherheit (ENISA) um Unterstützung bei der Einsetzung nationaler CSIRTs ersuchen.	(25) In Bezug auf personenbezogene Daten sollten CSIRTs in der Lage sein, im Einklang mit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[19] ***und der Richtlinie 2002/58/EG*** im Namen und auf Ersuchen einer unter die vorliegende Richtlinie fallenden Einrichtung eine ***Sicherheitsüberprüfung*** der für die Bereitstellung ihrer Dienste verwendeten ***Informationssysteme*** und ***Netzbereiche vorzunehmen, um spezifische Bedrohungen zu erkennen, abzuschwächen oder zu verhindern***. Die Mitgliedstaaten sollten für alle sektorbezogenen CSIRTs ein vergleichbares Niveau an technischen Kapazitäten anstreben. Die Mitgliedstaaten können die Agentur der Europäischen Union für Cybersicherheit (ENISA) um Unterstützung bei der Einsetzung nationaler CSIRTs ersuchen. ***Ferner sollten Cybersicherheitsrisiken niemals als Vorwand für Verletzungen der Grundrechte herangezogen werden.***

[19] Verordnung (EU) 2016/679 des

[19] Verordnung (EU) 2016/679 des

Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

Änderungsantrag 19

Vorschlag für eine Richtlinie
Erwägung 27

Vorschlag der Kommission	*Geänderter Text*
(27) Im Einklang mit dem Anhang der Empfehlung (EU) 2017/1548 der Kommission für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen („Konzeptentwurf“)[20] sollte der Begriff „Sicherheitsvorfall großen Ausmaßes“ einen Sicherheitsvorfall bezeichnen, der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat oder der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt. Je nach Ursache und Auswirkung können sich Sicherheitsvorfälle großen Ausmaßes verschärfen und zu echten Krisen entwickeln, die das reibungslose Funktionieren des Binnenmarkts verhindern. Angesichts der großen Tragweite und des, in den meisten Fällen, grenzübergreifenden Charakters solcher Sicherheitsvorfälle sollten die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union auf technischer, operativer und politischer Ebene zusammenarbeiten, um die Reaktion unionsweit angemessen zu koordinieren.	(27) Im Einklang mit dem Anhang der Empfehlung (EU) 2017/1548 der Kommission für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen („Konzeptentwurf“)[20] sollte der Begriff „Sicherheitsvorfall großen Ausmaßes“ einen Sicherheitsvorfall bezeichnen, der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat oder der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt. Je nach Ursache und Auswirkung können sich Sicherheitsvorfälle großen Ausmaßes verschärfen und zu echten Krisen entwickeln, die das reibungslose Funktionieren des Binnenmarkts verhindern ***oder ernsthafte Risiken für die öffentliche Sicherheit in mehreren Mitgliedstaaten oder der gesamten Union darstellen***. Angesichts der großen Tragweite und des, in den meisten Fällen, grenzübergreifenden Charakters solcher Sicherheitsvorfälle sollten die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union auf technischer, operativer und politischer Ebene zusammenarbeiten, um die Reaktion unionsweit angemessen zu koordinieren. ***Die Mitgliedstaaten müssen die***

	Umsetzung der EU-Vorschriften überwachen, sich bei grenzübergreifenden Problemen gegenseitig unterstützen, einen strukturierteren Dialog mit der Privatwirtschaft einrichten und bei Sicherheitsrisiken und Bedrohungen im Zusammenhang mit den neuen Technologien zusammenarbeiten, wie dies auch beim Thema 5G der Fall war.
[20] Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (ABl. L 239 vom 19.9.2017, S. 36).	[20] Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (ABl. L 239 vom 19.9.2017, S. 36).

Änderungsantrag 20

Vorschlag für eine Richtlinie
Erwägung 33

Vorschlag der Kommission	*Geänderter Text*
(33) Bei der Ausarbeitung von Leitfäden sollte die Kooperationsgruppe konsequent nationale Lösungen und Erfahrungen erfassen, die Auswirkungen ihrer Vorgaben auf nationale Ansätze bewerten, Herausforderungen bei der Umsetzung erörtern und spezifische Empfehlungen für eine bessere Umsetzung bestehender Vorschriften formulieren.	(33) Bei der Ausarbeitung von Leitfäden sollte die Kooperationsgruppe konsequent nationale ***und sektorspezifische*** Lösungen und Erfahrungen erfassen, die Auswirkungen ihrer Vorgaben auf nationale ***und sektorspezifische*** Ansätze bewerten, Herausforderungen bei der Umsetzung erörtern und spezifische Empfehlungen für eine bessere Umsetzung bestehender Vorschriften formulieren.

Änderungsantrag 21

Vorschlag für eine Richtlinie
Erwägung 34

Vorschlag der Kommission	*Geänderter Text*
(34) Die Kooperationsgruppe sollte ein flexibles Forum bleiben und in der Lage sein, unter Berücksichtigung der verfügbaren Ressourcen auf sich ändernde	(34) Die Kooperationsgruppe sollte ein flexibles Forum bleiben und in der Lage sein, unter Berücksichtigung der verfügbaren Ressourcen auf sich ändernde

und neue politische Prioritäten und Herausforderungen zu reagieren. Sie sollte regelmäßige gemeinsame Sitzungen mit einschlägigen privaten Interessenträgern aus der gesamten Union organisieren, um die Tätigkeiten der Gruppe zu erörtern und Beiträge zu neuen politischen Herausforderungen einzuholen. Um die Zusammenarbeit auf Unionsebene zu verbessern, sollte die Gruppe ***in Erwägung ziehen***, mit Cybersicherheitspolitik befasste Einrichtungen und Agenturen der Union, ***etwa das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3)***, die Agentur der Europäischen Union für Flugsicherheit (EASA) und die Agentur der Europäischen Union für das Weltraumprogramm (EUSPA), zur Teilnahme an ihrer Arbeit ***einzuladen***.

und neue politische Prioritäten und Herausforderungen zu reagieren. Sie sollte regelmäßige gemeinsame Sitzungen mit einschlägigen privaten Interessenträgern aus der gesamten Union organisieren, um die Tätigkeiten der Gruppe zu erörtern und Beiträge zu neuen politischen Herausforderungen einzuholen. Um die Zusammenarbeit auf Unionsebene zu verbessern, sollte die Gruppe ***einschlägige***, mit Cybersicherheitspolitik befasste Einrichtungen und Agenturen der Union, ***insbesondere Europol***, die Agentur der Europäischen Union für Flugsicherheit (EASA) und die Agentur der Europäischen Union für das Weltraumprogramm (EUSPA), zur Teilnahme an ihrer Arbeit ***einladen***.

Änderungsantrag 22

Vorschlag für eine Richtlinie
Erwägung 36

Vorschlag der Kommission	*Geänderter Text*
(36) Die Union sollte gegebenenfalls internationale Übereinkünfte mit Drittländern oder internationalen Organisationen im Einklang mit Artikel 218 AEUV schließen, in denen deren Beteiligung an bestimmten Tätigkeiten der Kooperationsgruppe und dem CSIRT-Netzwerk ermöglicht und geregelt wird. ***Solche Übereinkünfte sollten einen angemessenen Datenschutz gewährleisten***.	(36) Die Union sollte gegebenenfalls internationale Übereinkünfte mit Drittländern oder internationalen Organisationen im Einklang mit Artikel 218 AEUV schließen, in denen deren Beteiligung an bestimmten Tätigkeiten der Kooperationsgruppe und dem CSIRT-Netzwerk ermöglicht und geregelt wird. ***Soweit personenbezogene Daten an Drittländer oder an internationale Organisationen übermittelt werden, sollte Kapitel V der Verordnung (EU) 2016/679 Anwendung finden***.

Änderungsantrag 23

Vorschlag für eine Richtlinie
Erwägung 37

Vorschlag der Kommission	*Geänderter Text*
(37) Die Mitgliedstaaten sollten über die bestehenden Kooperationsnetzwerke – insbesondere das Netzwerk der Verbindungsorganisationen für Cyberkrisen (Cyber Crisis Liaison Organisation Network, EU-CyCLONe), das CSIRT-Netzwerk und die Kooperationsgruppe – zur Schaffung des EU-Rahmens für die Reaktion auf Cybersicherheitskrisen gemäß der Empfehlung (EU) 2017/1584 beitragen. EU-CyCLONe und das CSIRT-Netzwerk sollten auf der Grundlage von verfahrenstechnischen Vereinbarungen zusammenarbeiten, in denen die Modalitäten dieser Zusammenarbeit festgelegt werden. In der Geschäftsordnung von EU-CyCLONe sollten die Modalitäten für das Funktionieren des Netzwerks genauer festgelegt werden, einschließlich, aber nicht beschränkt auf Funktion und Aufgaben, Formen der Zusammenarbeit, Interaktionen mit anderen relevanten Akteuren und Vorlagen für den Informationsaustausch sowie Kommunikationsmittel. Für das Krisenmanagement auf Unionsebene sollten sich die relevanten Parteien auf die Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) stützen. Die Kommission sollte zu diesem Zweck auf den sektorübergreifenden Krisenkoordinierungsprozess auf hoher Ebene, ARGUS, zurückgreifen. Berührt die Krise eine wichtige externe Dimension oder eine Dimension der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP), so sollte der Krisenreaktionsmechanismus des Europäischen Auswärtigen Dienstes (EAD) ausgelöst werden.	(37) Die Mitgliedstaaten sollten über die bestehenden Kooperationsnetzwerke – insbesondere das Netzwerk der Verbindungsorganisationen für Cyberkrisen (Cyber Crisis Liaison Organisation Network, EU-CyCLONe), das CSIRT-Netzwerk und die Kooperationsgruppe – zur Schaffung des EU-Rahmens für die Reaktion auf Cybersicherheitskrisen gemäß der Empfehlung (EU) 2017/1584 beitragen. EU-CyCLONe und das CSIRT-Netzwerk sollten auf der Grundlage von verfahrenstechnischen Vereinbarungen zusammenarbeiten, in denen die Modalitäten dieser Zusammenarbeit festgelegt werden. In der Geschäftsordnung von EU-CyCLONe sollten die Modalitäten für das Funktionieren des Netzwerks genauer festgelegt werden, einschließlich, aber nicht beschränkt auf Funktion und Aufgaben, Formen der Zusammenarbeit, Interaktionen mit anderen relevanten Akteuren und Vorlagen für den Informationsaustausch sowie Kommunikationsmittel. Für das Krisenmanagement auf Unionsebene sollten sich die relevanten Parteien auf die Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) stützen. Die Kommission sollte zu diesem Zweck auf den sektorübergreifenden Krisenkoordinierungsprozess auf hoher Ebene, ARGUS, zurückgreifen. ***Wenn die Krise zwei oder mehr Mitgliedstaaten betrifft und mutmaßlichen kriminellen Hintergrund hat, sollte die Aktivierung des Notfallprotokolls der EU für die Reaktion der Strafverfolgungsbehörden in Betracht gezogen werden.*** Berührt die Krise eine wichtige externe Dimension oder eine Dimension der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP), so sollte der Krisenreaktionsmechanismus des Europäischen Auswärtigen Dienstes (EAD)

ausgelöst werden.

Änderungsantrag 24

Vorschlag für eine Richtlinie
Erwägung 45

Vorschlag der Kommission	*Geänderter Text*
(45) Die Einrichtungen sollten sich auch mit Cybersicherheitsrisiken befassen, die sich aus ihren Interaktionen und Beziehungen zu anderen interessierten Kreisen in einem weiter gefassten Ökosystem ergeben. Insbesondere sollten die Einrichtungen durch geeignete Maßnahmen sicherstellen, dass ihre Zusammenarbeit mit Hochschul- und Forschungseinrichtungen ihrer Cybersicherheitsstrategie entspricht und dabei bewährte Verfahren befolgt werden, was den sicheren Zugang zu sowie die Verbreitung von Informationen im Allgemeinen und den Schutz des geistigen Eigentums im Besonderen angeht. Auch sollten in Anbetracht der Bedeutung und des Wertes von Daten für die Tätigkeiten der Einrichtungen letztere alle geeigneten Cybersicherheitsmaßnahmen ergreifen, wenn sie die Datenverarbeitungs- und -analysedienste Dritter in Anspruch nehmen.	(45) Die Einrichtungen sollten sich auch mit Cybersicherheitsrisiken befassen, die sich aus ihren Interaktionen und Beziehungen zu anderen interessierten Kreisen in einem weiter gefassten Ökosystem ergeben. Insbesondere sollten die Einrichtungen durch geeignete Maßnahmen sicherstellen, dass ihre Zusammenarbeit mit Hochschul- und Forschungseinrichtungen ihrer Cybersicherheitsstrategie entspricht und dabei bewährte Verfahren befolgt werden, was den sicheren Zugang zu sowie die Verbreitung von Informationen im Allgemeinen und den Schutz des geistigen Eigentums im Besonderen angeht. Auch sollten in Anbetracht der Bedeutung und des Wertes von Daten für die Tätigkeiten der Einrichtungen letztere alle geeigneten Cybersicherheitsmaßnahmen ergreifen, wenn sie die Datenverarbeitungs- und -analysedienste Dritter in Anspruch nehmen***, und potenzielle Cyberangriffe, die sie feststellen, melden***.

Änderungsantrag 25

Vorschlag für eine Richtlinie
Erwägung 46 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(46a) Besondere Aufmerksamkeit sollte dem Umstand gewidmet werden, dass IKT-Dienste, -Systeme oder -Produkte in ihrem Ursprungsland besonderen Anforderungen unterliegen, die ein Hindernis für die Einhaltung der EU-

Rechtsvorschriften über die Privatsphäre und den Datenschutz darstellen könnten. Im Rahmen derartiger Risikobewertungen sollte gegebenenfalls der EDSA konsultiert werden. Freie und quelloffene Software sowie quelloffene Hardware könnten in Bezug auf die Cybersicherheit enorme Vorteile bieten, was die Transparenz und die Überprüfbarkeit von Merkmalen betrifft. Da dies dazu beitragen könnte, bestimmte Risiken in der Lieferkette anzugehen und zu mindern, sollte ihrer Verwendung nach Möglichkeit im Einklang mit der Stellungnahme 5/2021 des EDSB[1a] Vorrang eingeräumt werden.

[1a] Stellungnahme 5/2021 des Europäischen Datenschutzbeauftragten zur Cybersicherheitsstrategie und zur NIS-2-Richtlinie, 11. März 2021.

Änderungsantrag 26

Vorschlag für eine Richtlinie
Erwägung 47

Vorschlag der Kommission	*Geänderter Text*
(47) Bei den Lieferketten-Risikobewertungen unter Berücksichtigung der Besonderheiten des jeweiligen Sektors sollte sowohl technischen wie auch gegebenenfalls nichttechnischen Faktoren Rechnung getragen werden, ***einschließlich derer***, die in der Empfehlung (EU) 2019/534, in der EU-weit koordinierten Risikobewertung zur Cybersicherheit in 5G-Netzen sowie in dem von der Kooperationsgruppe vereinbarten EU-Instrumentarium für die 5G-Cybersicherheit definiert sind. Bei der Ermittlung der Lieferketten, die einer koordinierten Risikobewertung unterzogen werden sollten, sollten folgende Kriterien berücksichtigt werden: i) der Umfang, in dem wesentliche und wichtige	(47) Bei den Lieferketten-Risikobewertungen unter Berücksichtigung der Besonderheiten des jeweiligen Sektors sollte sowohl technischen wie auch gegebenenfalls nichttechnischen Faktoren Rechnung getragen werden, ***die von der Koordinierungsgruppe näher festgelegt werden sollten und zu denen die Faktoren gehören***, die in der Empfehlung (EU) 2019/534, in der EU-weit koordinierten Risikobewertung zur Cybersicherheit in 5G-Netzen sowie in dem von der Kooperationsgruppe vereinbarten EU-Instrumentarium für die 5G-Cybersicherheit definiert sind. Bei der Ermittlung der Lieferketten, die einer koordinierten Risikobewertung unterzogen werden sollten, sollten folgende Kriterien

Einrichtungen bestimmte kritische IKT-Dienste, -Systeme oder -Produkte nutzen und auf sie angewiesen sind; ii) die Bedeutung bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte für die Ausführung kritischer oder sensibler Funktionen, einschließlich der Verarbeitung personenbezogener Daten; iii) die Verfügbarkeit alternativer IKT-Dienste, -Systeme oder -Produkte; iv) die Resilienz der gesamten Lieferkette von IKT-Diensten, -Systemen oder -Produkten gegen destabilisierende Ereignisse und v) die potenzielle künftige Bedeutung neuer IKT-Dienste, -Systeme oder -Produkte für die Tätigkeiten der Einrichtungen.	berücksichtigt werden: i) der Umfang, in dem wesentliche und wichtige Einrichtungen bestimmte kritische IKT-Dienste, -Systeme oder -Produkte nutzen und auf sie angewiesen sind; ii) die Bedeutung bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte für die Ausführung kritischer oder sensibler Funktionen, einschließlich der Verarbeitung personenbezogener Daten; iii) die Verfügbarkeit alternativer IKT-Dienste, -Systeme oder -Produkte; iv) die Resilienz der gesamten Lieferkette von IKT-Diensten, -Systemen oder -Produkten gegen destabilisierende Ereignisse und v) die potenzielle künftige Bedeutung neuer IKT-Dienste, -Systeme oder -Produkte für die Tätigkeiten der Einrichtungen.

Änderungsantrag 27

Vorschlag für eine Richtlinie
Erwägung 48 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(48a) Kleine und mittlere Unternehmen (KMU) sind oft nicht groß genug und verfügen nicht über genügend Ressourcen, um in einer vernetzten Welt, in der die Telearbeit zunimmt, eine breite und zunehmende Palette an Cybersicherheitsanforderungen zu erfüllen. Die Mitgliedstaaten sollten daher in ihren nationalen Cybersicherheitsstrategien Leitlinien und Unterstützung für KMU vorsehen.

Änderungsantrag 28

Vorschlag für eine Richtlinie
Erwägung 50

Vorschlag der Kommission	*Geänderter Text*
(50) Angesichts der wachsenden Bedeutung nummernunabhängiger interpersoneller Kommunikationsdienste	(50) Angesichts der wachsenden Bedeutung nummernunabhängiger interpersoneller Kommunikationsdienste

muss sichergestellt werden, dass auch für diese Dienste angemessene Sicherheitsanforderungen entsprechend ihrer spezifischen Art und wirtschaftlichen Bedeutung gelten. Die Anbieter solcher Dienste sollten daher auch ein ***Sicherheitsniveau von Netz- und Informationssystemen*** gewährleisten, das dem bestehenden Risiko angemessen ist. Da die Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste üblicherweise keine tatsächliche Kontrolle über die Signalübertragung über Netze ausüben, kann das Risiko für solche Dienste in gewisser Hinsicht als geringer erachtet werden als für herkömmliche elektronische Kommunikationsdienste. Dasselbe gilt auch für interpersonelle Kommunikationsdienste, die Nummern nutzen und die keine tatsächliche Kontrolle über die Signalübertragung ausüben.	muss sichergestellt werden, dass auch für diese Dienste angemessene Sicherheitsanforderungen entsprechend ihrer spezifischen Art und wirtschaftlichen Bedeutung gelten. Die Anbieter solcher Dienste sollten daher auch ein ***Cybersicherheitsniveau*** gewährleisten, das dem bestehenden Risiko angemessen ist. Da die Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste üblicherweise keine tatsächliche Kontrolle über die Signalübertragung über Netze ausüben, kann das Risiko für solche Dienste in gewisser Hinsicht als geringer erachtet werden als für herkömmliche elektronische Kommunikationsdienste. Dasselbe gilt auch für interpersonelle Kommunikationsdienste, die Nummern nutzen und die keine tatsächliche Kontrolle über die Signalübertragung ausüben.

Änderungsantrag 29

Vorschlag für eine Richtlinie
Erwägung 52

Vorschlag der Kommission	*Geänderter Text*
(52) Gegebenenfalls sollten die Einrichtungen die Empfänger ihrer Dienste über besondere und erhebliche Bedrohungen sowie über Maßnahmen informieren, die sie ergreifen können, um das sich daraus ergebende Risiko für sich selbst zu mindern. Die Verpflichtung zur Information der Empfänger über solche Bedrohungen sollte die Einrichtungen nicht von der Pflicht befreien, auf eigene Kosten angemessene Sofortmaßnahmen zu ergreifen, um jedwede Cyberbedrohung zu verhüten oder zu beseitigen und das normale Sicherheitsniveau des Dienstes wiederherzustellen. Die Bereitstellung solcher Informationen über Sicherheitsbedrohungen sollte für die Empfänger kostenlos sein.	(52) Gegebenenfalls sollten die Einrichtungen ***in der Lage sein,*** die Empfänger ihrer Dienste über besondere und erhebliche Bedrohungen sowie über Maßnahmen ***zu*** informieren, die sie ergreifen können, um das sich daraus ergebende Risiko für sich selbst zu mindern. Die Verpflichtung zur Information der Empfänger über solche Bedrohungen sollte die Einrichtungen nicht von der Pflicht befreien, auf eigene Kosten angemessene Sofortmaßnahmen zu ergreifen, um jedwede Cyberbedrohung zu verhüten oder zu beseitigen und das normale Sicherheitsniveau des Dienstes wiederherzustellen. Die Bereitstellung solcher Informationen über Sicherheitsbedrohungen sollte für die Empfänger kostenlos sein.

Änderungsantrag 30

Vorschlag für eine Richtlinie
Erwägung 53

Vorschlag der Kommission	*Geänderter Text*
(53) Insbesondere sollten die Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste die Empfänger der Dienste über besondere und erhebliche Cyberbedrohungen sowie über Maßnahmen zum Schutz ***von Kommunikationsinhalten***, die sie treffen können, informieren, z. B. den Einsatz spezieller Software oder von Verschlüsselungsverfahren.	(53) Insbesondere sollten die Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste die ***Grundsätze der eingebauten Sicherheit und der Sicherheit durch Voreinstellungen umsetzen und in der Lage sein, die*** Empfänger der Dienste über besondere und erhebliche Cyberbedrohungen sowie über Maßnahmen zum Schutz ***ihrer Geräte und Kommunikationsinhalte***, die sie treffen können, ***zu*** informieren, z. B. den Einsatz spezieller Software oder von Verschlüsselungsverfahren. ***Um die Sicherheit der Hardware und Software zu erhöhen, sollten die Anbieter darin bestärkt werden, Open-Source-Hardware zu verwenden.***

Änderungsantrag 31

Vorschlag für eine Richtlinie
Erwägung 54

Vorschlag der Kommission	*Geänderter Text*
(54) Zur Aufrechterhaltung der Sicherheit elektronischer Kommunikationsnetze und -dienste sollte die Verschlüsselung, insbesondere von Ende zu Ende, gefördert werden; erforderlichenfalls sollte sie für die Anbieter solcher Dienste und Netze im Einklang mit den Grundsätzen der Sicherheit und des Schutzes der Privatsphäre mittels datenschutzfreundlicher Voreinstellungen und Technikgestaltung für die Zwecke des	(54) Zur Aufrechterhaltung der Sicherheit elektronischer Kommunikationsnetze und -dienste ***und zum Schutz der Grundrechte auf Datenschutz und Schutz der Privatsphäre*** sollte die Verschlüsselung, insbesondere von Ende zu Ende, gefördert werden; erforderlichenfalls sollte sie für die Anbieter solcher Dienste und Netze im Einklang mit den Grundsätzen der Sicherheit und des Schutzes der Privatsphäre mittels

Artikels 18 vorgeschrieben werden. Die Nutzung der End-zu-End-Verschlüsselung sollte mit ***den Befugnissen*** der Mitgliedstaaten, den Schutz ihrer wesentlichen Sicherheitsinteressen und der öffentlichen Sicherheit zu gewährleisten und die ***Ermittlung***, Aufdeckung und Verfolgung von Straftaten im Einklang mit dem Unionsrecht zu ermöglichen, in Einklang gebracht werden. Lösungen für den rechtmäßigen Zugang zu Informationen in End-zu-End-verschlüsselter Kommunikation sollten die Wirksamkeit der Verschlüsselung beim Schutz der Privatsphäre und der Sicherheit der Kommunikation aufrechterhalten und ***zugleich eine wirksame Reaktion*** auf ***Straftaten gewährleisten***.

datenschutzfreundlicher Voreinstellungen und Technikgestaltung für die Zwecke des Artikels 18 vorgeschrieben werden. Die Nutzung der End-zu-End-Verschlüsselung sollte mit ***der Zuständigkeit*** der Mitgliedstaaten ***dafür***, den Schutz ihrer wesentlichen Sicherheitsinteressen und der öffentlichen Sicherheit zu gewährleisten und die ***Verhütung***, Aufdeckung und Verfolgung von Straftaten im Einklang mit dem Unionsrecht ***und dem nationalen Recht*** zu ermöglichen, in Einklang gebracht werden. Lösungen für den rechtmäßigen Zugang zu Informationen in End-zu-End-verschlüsselter Kommunikation sollten die Wirksamkeit der Verschlüsselung beim Schutz der Privatsphäre und der Sicherheit der Kommunikation aufrechterhalten***. Keine Bestimmung in dieser Verordnung sollte als Versuch, die End-zu-End-Verschlüsselung durch „Hintertüren“ oder ähnliche Lösungen zu schwächen, angesehen werden, da Mängel bei der Verschlüsselung für böswillige Zwecke ausgenutzt werden könnten. Jede Maßnahme mit dem Ziel, die Verschlüsselung zu schwächen oder die Architektur der Technologie zu umgehen, könnte erhebliche Risiken für die damit verbundenen wirksamen Schutzkapazitäten zur Folge haben. Jede unautorisierte Entschlüsselung oder Überwachung elektronischer Kommunikation, die nicht von Justizbehörden vorgenommen wird, sollte verboten werden, um die Wirksamkeit der Technologie*** und ***ihre umfassendere Nutzung sicherzustellen. Es ist wichtig, dass sich die Mitgliedstaaten mit Problemen befassen, mit denen Justizbehörden und Forscher, die sich mit Schwachstellen beschäftigen, konfrontiert sind. In einigen Mitgliedstaaten können Einrichtungen und natürliche Personen, die Forschung zu Schwachstellen betreiben, strafrechtlich und zivilrechtlich zur Verantwortung gezogen werden. Die Mitgliedstaaten werden daher***

aufgefordert, Leitlinien für den Verzicht auf Strafverfolgung und die Nichthaftung in Bezug auf Forschung im Bereich der Informationssicherheit herauszugeben.

Änderungsantrag 32

Vorschlag für eine Richtlinie
Erwägung 56

Vorschlag der Kommission	*Geänderter Text*
(56) Wesentliche und wichtige Einrichtungen sind häufig in einer Situation, in der ein bestimmter Sicherheitsvorfall aufgrund seiner Merkmale und sich aus verschiedenen Rechtsinstrumenten ergebender Meldepflichten verschiedenen Behörden gemeldet werden muss. Solche Fälle führen zu zusätzlichen Belastungen und unter Umständen auch zu Unsicherheiten hinsichtlich des Formats solcher Meldungen und der für sie geltenden Verfahren. Vor diesem Hintergrund und zur Vereinfachung der Meldung von Sicherheitsvorfällen sollten die Mitgliedstaaten eine zentrale Anlaufstelle ***für alle Meldungen*** einrichten, die aufgrund dieser Richtlinie sowie anderer EU-Rechtsvorschriften wie der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG vorgeschrieben ***sind***. Die ENISA sollte in Zusammenarbeit mit der Kooperationsgruppe mittels Leitlinien einheitliche Meldemuster erstellen, die die im Unionsrecht geforderten Informationen vereinfachen und straffen und den Aufwand für die Unternehmen verringern würden.	(56) Wesentliche und wichtige Einrichtungen sind häufig in einer Situation, in der ein bestimmter Sicherheitsvorfall aufgrund seiner Merkmale und sich aus verschiedenen Rechtsinstrumenten ergebender Meldepflichten verschiedenen Behörden gemeldet werden muss. Solche Fälle führen zu zusätzlichen Belastungen und unter Umständen auch zu Unsicherheiten hinsichtlich des Formats solcher Meldungen und der für sie geltenden Verfahren. Vor diesem Hintergrund und zur Vereinfachung der Meldung von Sicherheitsvorfällen sollten die Mitgliedstaaten eine zentrale Anlaufstelle einrichten, die aufgrund dieser Richtlinie sowie anderer EU-Rechtsvorschriften wie der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG vorgeschrieben ***ist***. Die ENISA sollte in Zusammenarbeit mit der Kooperationsgruppe ***und dem Europäischen Datenschutzausschuss*** mittels Leitlinien einheitliche Meldemuster erstellen, die die im Unionsrecht geforderten Informationen vereinfachen und straffen und den Aufwand für die Unternehmen verringern würden.

Änderungsantrag 33

Vorschlag für eine Richtlinie
Erwägung 57

Vorschlag der Kommission	*Geänderter Text*
(57) Wenn der Verdacht besteht, dass ein Sicherheitsvorfall im Zusammenhang mit schweren kriminellen Handlungen nach Unionsrecht oder nationalem Recht steht, sollten die Mitgliedstaaten wesentliche und wichtige Einrichtungen – auf der Grundlage geltender strafverfahrensrechtlicher Bestimmungen im Einklang mit dem Unionsrecht – dazu anhalten, diese Sicherheitsvorfälle mit einem mutmaßlichen schwerwiegenden kriminellen Hintergrund den zuständigen Strafverfolgungsbehörden zu melden. Unbeschadet der für Europol geltenden Vorschriften für den Schutz personenbezogener Daten ist gegebenenfalls die Unterstützung durch ***das*** EC3 und die ENISA bei der Koordinierung zwischen den zuständigen Behörden und den Strafverfolgungsbehörden verschiedener Mitgliedstaaten wünschenswert.	(57) Wenn der Verdacht besteht, dass ein Sicherheitsvorfall im Zusammenhang mit schweren kriminellen Handlungen nach Unionsrecht oder nationalem Recht steht, sollten die Mitgliedstaaten wesentliche und wichtige Einrichtungen – auf der Grundlage geltender strafverfahrensrechtlicher Bestimmungen im Einklang mit dem Unionsrecht – dazu anhalten, diese Sicherheitsvorfälle mit einem mutmaßlichen schwerwiegenden kriminellen Hintergrund den zuständigen Strafverfolgungsbehörden zu melden. Unbeschadet der für Europol geltenden Vorschriften für den Schutz personenbezogener Daten ist gegebenenfalls die Unterstützung durch ***Europols Europäisches Zentrum zur Bekämpfung der Cyberkriminalität (***EC3***)*** und die ENISA bei der Koordinierung zwischen den zuständigen Behörden und den Strafverfolgungsbehörden verschiedener Mitgliedstaaten wünschenswert.

Änderungsantrag 34

Vorschlag für eine Richtlinie
Erwägung 58

Vorschlag der Kommission	*Geänderter Text*
(58) Häufig ist bei Sicherheitsvorfällen der Schutz personenbezogener Daten nicht mehr gewährleistet. In diesem Zusammenhang sollten die zuständigen Behörden gemäß der Richtlinie 2002/58/EG mit den Datenschutzbehörden und den Aufsichtsbehörden zusammenarbeiten und Informationen über alle relevanten Angelegenheiten austauschen.	(58) Häufig ist bei Sicherheitsvorfällen der Schutz personenbezogener Daten nicht mehr gewährleistet. In diesem Zusammenhang sollten die zuständigen Behörden gemäß der ***Verordnung (EU) 2016/679 und der*** Richtlinie 2002/58/EG mit den Datenschutzbehörden und den Aufsichtsbehörden zusammenarbeiten und Informationen über alle relevanten Angelegenheiten austauschen.

Änderungsantrag 35

Vorschlag für eine Richtlinie
Erwägung 59

Vorschlag der Kommission	*Geänderter Text*
(59) Die Pflege genauer und vollständiger Datenbanken mit Domänennamen und Registrierungsdaten (sogenannte „WHOIS-Daten“) und ein rechtmäßiger Zugang zu diesen Daten sind entscheidend, um die Sicherheit, Stabilität und Resilienz des DNS zu gewährleisten, was wiederum zu einem hohen gemeinsamen Cybersicherheitsniveau in der Union beiträgt. Werden auch personenbezogene Daten verarbeitet, so muss diese Verarbeitung mit dem EU-Datenschutzrecht im Einklang stehen.	(59) Die Pflege genauer und vollständiger Datenbanken mit Domänennamen und Registrierungsdaten (sogenannte „WHOIS-Daten“) und ein rechtmäßiger Zugang zu diesen Daten sind entscheidend, um die Sicherheit, Stabilität und Resilienz des DNS zu gewährleisten, was wiederum zu einem hohen gemeinsamen Cybersicherheitsniveau in der Union beiträgt. Werden auch personenbezogene Daten verarbeitet, so muss diese Verarbeitung mit dem ***geltenden*** EU-Datenschutzrecht im Einklang stehen.

Änderungsantrag 36

Vorschlag für eine Richtlinie
Erwägung 62

Vorschlag der Kommission	*Geänderter Text*
(62) ***TLD-Register*** und die Einrichtungen, die Domänennamen-Registrierungsdienste für sie erbringen, ***sollten*** Domänennamen-Registrierungsdaten, die ***nicht*** den ***EU-Datenschutzvorschriften unterliegen, z. B. Daten***, ***die juristische Personen betreffen[25],*** öffentlich zugänglich machen. TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, sollten es auch ermöglichen, dass berechtigte Zugangsnachfrager ***rechtmäßigen Zugang zu bestimmten Domänennamen-Registrierungsdaten natürlicher Personen*** im Einklang mit ***dem EU-Datenschutzrecht*** erhalten. Die Mitgliedstaaten sollten sicherstellen, dass TLD-Register und die Einrichtungen, die	(62) ***Um eine rechtliche Verpflichtung im Sinne von Artikel 6 Absatz 1 Buchstabe c und Artikel 6 Absatz 3 der Verordnung (EU) 2016/679 zu erfüllen, sollten TLD-Register*** und die Einrichtungen, die Domänennamen-Registrierungsdienste für sie erbringen, ***bestimmte*** Domänennamen-Registrierungsdaten, die ***in*** den ***für sie geltenden Rechtsvorschriften der Mitgliedstaaten festgelegt sind***, ***wie den Domänennamen und den Namen der juristischen Person*** öffentlich zugänglich machen. TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, sollten es auch ermöglichen, dass berechtigte Zugangsnachfrager – ***insbesondere zuständige Behörden gemäß***

Domänennamen-Registrierungsdienste für sie erbringen, Anträge ***berechtigter Zugangsnachfrager*** auf Offenlegung von Domänennamen-Registrierungsdaten unverzüglich beantworten. TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für sie erbringen, sollten Grundsätze und Verfahren für die Veröffentlichung und Offenlegung von Registrierungsdaten festlegen, einschließlich Leistungsvereinbarungen für die Bearbeitung von Anträgen berechtigter Zugangsnachfrager. Das Zugangsverfahren kann auch die Verwendung einer Schnittstelle, eines Portals oder eines anderen technischen Instruments umfassen, um ein effizientes System für die Anforderung von und den Zugriff auf Registrierungsdaten bereitzustellen. Zur Förderung einheitlicher Verfahren für den gesamten Binnenmarkt kann die Kommission unbeschadet der Zuständigkeiten des Europäischen Datenschutzausschusses Leitlinien zu solchen Verfahren erlassen.

der vorliegenden Richtlinie oder Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 im Einklang mit ***ihren Befugnissen – rechtmäßigen Zugang zu bestimmten Domänennamen-Registrierungsdaten natürlicher Personen*** erhalten. Die Mitgliedstaaten sollten sicherstellen, dass TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für sie erbringen, ***rechtmäßige und hinreichend begründete*** Anträge ***von Behörden – einschließlich zuständiger Behörden gemäß dieser Richtlinie, nach Unionsrecht oder nationalem Recht für die Verhütung, Ermittlung oder Verfolgung von Straftaten zuständiger Behörden und Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 –*** auf Offenlegung von Domänennamen-Registrierungsdaten unverzüglich beantworten. TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für sie erbringen, sollten Grundsätze und Verfahren für die Veröffentlichung und Offenlegung von Registrierungsdaten festlegen, einschließlich Leistungsvereinbarungen für die Bearbeitung von Anträgen berechtigter Zugangsnachfrager ***auf Zugang***. Das Zugangsverfahren kann auch die Verwendung einer Schnittstelle, eines Portals oder eines anderen technischen Instruments umfassen, um ein effizientes System für die Anforderung von und den Zugriff auf Registrierungsdaten bereitzustellen. Zur Förderung einheitlicher Verfahren für den gesamten Binnenmarkt kann die Kommission unbeschadet der Zuständigkeiten des Europäischen Datenschutzausschusses Leitlinien zu solchen Verfahren erlassen.

---

[25] Erwägungsgrund 14 der VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES: „Diese Verordnung gilt nicht für die Verarbeitung

personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person.“

Änderungsantrag 37

Vorschlag für eine Richtlinie
Erwägung 63

Vorschlag der Kommission	*Geänderter Text*
(63) ***Alle*** wesentlichen und wichtigen Einrichtungen, die unter diese Richtlinie fallen, ***sollten*** der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegen, in dem sie ihre Dienste erbringen. Erbringt die Einrichtung Dienste in mehreren Mitgliedstaaten, so sollte sie unter die getrennte und parallele gerichtliche Zuständigkeit der betreffenden Mitgliedstaaten fallen. Die zuständigen Behörden dieser Mitgliedstaaten sollten zusammenarbeiten, einander Amtshilfe leisten und gegebenenfalls gemeinsame Aufsichtstätigkeiten durchführen.	(63) ***Für die Zwecke dieser Richtlinie sollten alle*** wesentlichen und wichtigen Einrichtungen, die unter diese Richtlinie fallen, der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegen, in dem sie ihre Dienste erbringen. Erbringt die Einrichtung Dienste in mehreren Mitgliedstaaten, so sollte sie unter die getrennte und parallele gerichtliche Zuständigkeit der betreffenden Mitgliedstaaten fallen. Die zuständigen Behörden dieser Mitgliedstaaten sollten ***sich auf einzelne Klassifizierungen einigen, nach Möglichkeit*** zusammenarbeiten, einander ***in Echtzeit*** Amtshilfe leisten und gegebenenfalls gemeinsame Aufsichtstätigkeiten durchführen.

Änderungsantrag 38

Vorschlag für eine Richtlinie
Erwägung 64

Vorschlag der Kommission	*Geänderter Text*
(64) Da die Dienste und Tätigkeiten, die von DNS-Diensteanbietern, TLD-Namenregistern, Betreibern von Inhaltszustellnetzen, Anbietern von Cloud-Computing-Diensten sowie Anbietern von Rechenzentrumsdiensten und Anbietern digitaler Dienste erbracht werden, grenzübergreifenden Charakter haben, sollte jeweils immer nur ein Mitgliedstaat	(64) Da die Dienste und Tätigkeiten, die von DNS-Diensteanbietern, TLD-Namenregistern, Betreibern von Inhaltszustellnetzen, Anbietern von Cloud-Computing-Diensten sowie Anbietern von Rechenzentrumsdiensten und Anbietern digitaler Dienste erbracht werden, grenzübergreifenden Charakter haben, sollte jeweils immer nur ein Mitgliedstaat

für diese Einrichtungen zuständig sein. Die ***gerichtliche Zuständigkeit*** sollte bei dem Mitgliedstaat liegen, in dem die betreffende Einrichtung ihre Hauptniederlassung in der Union hat. Das Kriterium der Niederlassung im Sinne dieser Richtlinie setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei unerheblich. Dieses Kriterium sollte nicht davon abhängen, ob die Netz- und Informationssysteme an einem bestimmten Ort physisch untergebracht sind; die Existenz und die Nutzung derartiger Systeme stellen an sich keine derartige Hauptniederlassung dar und sind daher kein ausschlaggebendes Kriterium für die Bestimmung der Hauptniederlassung. Die Hauptniederlassung sollte der Ort sein, an dem in der Union über Maßnahmen des Cybersicherheitsrisikomanagements entschieden wird. In der Regel entspricht dies dem Ort, an dem sich die Hauptverwaltung der Unternehmen in der Union befindet. Werden solche Entscheidungen nicht in der Union getroffen, sollte davon ausgegangen werden, dass sich die Hauptniederlassung in dem Mitgliedstaat befindet, in dem die Einrichtung über eine Niederlassung mit der unionsweit höchsten Beschäftigtenzahl verfügt. Werden die Dienste von einer Unternehmensgruppe ausgeführt, so sollte die Hauptniederlassung des herrschenden Unternehmens als Hauptniederlassung der Unternehmensgruppe gelten.

für diese Einrichtungen zuständig sein. ***Für*** die ***Zwecke dieser Richtlinie*** sollte ***die gerichtliche Zuständigkeit*** bei dem Mitgliedstaat liegen, in dem die betreffende Einrichtung ihre Hauptniederlassung in der Union hat. Das Kriterium der Niederlassung im Sinne dieser Richtlinie setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei unerheblich. Dieses Kriterium sollte nicht davon abhängen, ob die Netz- und Informationssysteme an einem bestimmten Ort physisch untergebracht sind; die Existenz und die Nutzung derartiger Systeme stellen an sich keine derartige Hauptniederlassung dar und sind daher kein ausschlaggebendes Kriterium für die Bestimmung der Hauptniederlassung. Die Hauptniederlassung sollte der Ort sein, an dem in der Union über Maßnahmen des Cybersicherheitsrisikomanagements entschieden wird. In der Regel entspricht dies dem Ort, an dem sich die Hauptverwaltung der Unternehmen in der Union befindet. Werden solche Entscheidungen nicht in der Union getroffen, sollte davon ausgegangen werden, dass sich die Hauptniederlassung in dem Mitgliedstaat befindet, in dem die Einrichtung über eine Niederlassung mit der unionsweit höchsten Beschäftigtenzahl verfügt. Werden die Dienste von einer Unternehmensgruppe ausgeführt, so sollte die Hauptniederlassung des herrschenden Unternehmens als Hauptniederlassung der Unternehmensgruppe gelten.

Änderungsantrag 39

Vorschlag für eine Richtlinie
Erwägung 69

Vorschlag der Kommission	*Geänderter Text*
(69) Die Verarbeitung personenbezogener Daten durch Einrichtungen, Behörden, CERTs, CSIRTs sowie Anbieter von Sicherheitstechnologien und -diensten ***sollte im Sinne*** der Verordnung (EU) 2016/679 ein berechtigtes Interesse des jeweiligen Verantwortlichen ***darstellen, wie dies für die Gewährleistung*** der ***Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist***. Dies sollte auch Folgendes einschließen: Maßnahmen im Hinblick auf die Verhütung, Erkennung, Analyse und Bewältigung von Sicherheitsvorfällen, Maßnahmen zur Sensibilisierung für spezifische Cyberbedrohungen, Informationsaustausch im Zusammenhang mit der Behebung von Schwachstellen und ihrer koordinierten Offenlegung, freiwilliger Austausch von Informationen über solche Sicherheitsvorfälle sowie über Cyberbedrohungen und Schwachstellen, Gefährdungsindikatoren, Taktiken, Vorgehensweisen und Verfahren, Cybersicherheitswarnungen und Konfigurationstools. ***Diese*** Maßnahmen können die Verarbeitung ***folgender Arten*** personenbezogener Daten erfordern***:*** IP-Adressen, Uniform Resource Locators (URL-Adressen), Domänennamen und E-Mail-Adressen.	(69) Die Verarbeitung personenbezogener Daten durch Einrichtungen, Behörden, CERTs, CSIRTs sowie Anbieter von Sicherheitstechnologien und -diensten ***in dem Ausmaß, das für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, ist notwendig, damit sie ihre rechtlichen Verpflichtungen gemäß dem nationalen Recht zur Umsetzung dieser Richtlinie erfüllen und fällt somit unter Artikel 6 Absatz 1 Buchstabe c und Artikel 6 Absatz 3*** der Verordnung (EU) 2016/679***. Zudem sollte eine derartige Verarbeitung*** ein berechtigtes Interesse des jeweiligen Verantwortlichen ***im Sinne von Artikel 6 Absatz 1 Buchstabe f*** der ***Verordnung (EU) 2016/679 darstellen***. Dies sollte auch Folgendes einschließen: Maßnahmen im Hinblick auf die Verhütung, Erkennung, Analyse und Bewältigung von Sicherheitsvorfällen, Maßnahmen zur Sensibilisierung für spezifische Cyberbedrohungen, Informationsaustausch im Zusammenhang mit der Behebung von Schwachstellen und ihrer koordinierten Offenlegung, freiwilliger Austausch von Informationen über solche Sicherheitsvorfälle sowie über Cyberbedrohungen und Schwachstellen, Gefährdungsindikatoren, Taktiken, Vorgehensweisen und Verfahren, Cybersicherheitswarnungen und Konfigurationstools. ***Häufig ist der Schutz personenbezogener Daten nach Cybersicherheitsvorfällen nicht mehr gewährleistet; deswegen sollten die zuständigen Behörden und die Datenschutzbehörden der EU-Mitgliedstaaten zusammenarbeiten und Informationen über alle relevanten Angelegenheiten austauschen, um sich mit jeglicher Verletzung des Schutzes personenbezogener Daten zu befassen. Die*** Maßnahmen können die Verarbeitung

bestimmter Kategorien personenbezogener Daten erfordern***, einschließlich*** IP-Adressen, Uniform Resource Locators (URL-Adressen), Domänennamen und E-Mail-Adressen.

Änderungsantrag 40

Vorschlag für eine Richtlinie
Erwägung 71

Vorschlag der Kommission	*Geänderter Text*
(71) Für eine wirksame Durchsetzung sollte ein Mindestumfang von Verwaltungssanktionen für Verstöße gegen die Verpflichtungen im Bereich des Cybersicherheitsrisikomanagements und die Meldepflichten gemäß dieser Richtlinie festgelegt werden, womit für die gesamte Union ein klarer und kohärenter Rahmen für solche Sanktionen geschaffen wird. Folgendem sollte gebührend Rechnung getragen werden: der ***Art,*** Schwere und Dauer des Verstoßes, den tatsächlich entstandenen Schäden oder Verlusten bzw. den Schäden oder Verlusten, die hätten entstehen können, der Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, den Maßnahmen zur Vermeidung oder Minderung der entstandenen Schäden/Verluste, dem Grad der Verantwortlichkeit oder jeglichem früheren Verstoß, dem Umfang der Zusammenarbeit mit der ***Aufsichtsbehörde*** sowie jedem anderen erschwerenden oder mildernden Umstand. Für die ***Verhängung von*** Sanktionen einschließlich Geldbußen sollte es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta der Grundrechte der Europäischen Union, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, entsprechen.	(71) Für eine wirksame Durchsetzung sollte ein Mindestumfang von Verwaltungssanktionen für Verstöße gegen die Verpflichtungen im Bereich des Cybersicherheitsrisikomanagements und die Meldepflichten gemäß dieser Richtlinie festgelegt werden, womit für die gesamte Union ein klarer und kohärenter Rahmen für solche Sanktionen geschaffen wird. Folgendem sollte gebührend Rechnung getragen werden: der Schwere und Dauer des Verstoßes, den tatsächlich entstandenen Schäden oder Verlusten bzw. den Schäden oder Verlusten, die hätten entstehen können, ***etwaigen relevanten vorherigen Verstößen, der Art und Weise, in der die zuständige Behörde von dem Verstoß Kenntnis erlangt hat,*** der Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, den Maßnahmen zur Vermeidung oder Minderung der entstandenen Schäden/Verluste, dem Grad der Verantwortlichkeit oder jeglichem ***relevanten*** früheren Verstoß, dem Umfang der Zusammenarbeit mit der ***zuständigen Behörde*** sowie jedem anderen erschwerenden oder mildernden Umstand. Für die ***verhängten*** Sanktionen einschließlich Geldbußen sollte es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta der Grundrechte der Europäischen Union, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren,

entsprechen.

Änderungsantrag 41

Vorschlag für eine Richtlinie
Erwägung 74

Vorschlag der Kommission	*Geänderter Text*
(74) Die Mitgliedstaaten sollten die ***strafrechtlichen*** Sanktionen für Verstöße gegen die nationalen Vorschriften zur Umsetzung dieser Richtlinie festlegen können. Die Verhängung von strafrechtlichen Sanktionen für Verstöße gegen solche nationalen Vorschriften und von entsprechenden verwaltungsrechtlichen Sanktionen sollte jedoch nicht zu einer Verletzung des Grundsatzes „ne bis in idem“, wie er vom Gerichtshof ausgelegt worden ist, führen.	(74) Die Mitgliedstaaten sollten die ***Vorschriften über strafrechtliche*** Sanktionen für Verstöße gegen die nationalen Vorschriften zur Umsetzung dieser Richtlinie festlegen können***. Diese strafrechtlichen Sanktionen können auch die Einziehung der durch die Verstöße gegen diese Verordnung erzielten Gewinne ermöglichen***. Die Verhängung von strafrechtlichen Sanktionen für Verstöße gegen solche nationalen Vorschriften und von entsprechenden verwaltungsrechtlichen Sanktionen sollte jedoch nicht zu einer Verletzung des Grundsatzes „ne bis in idem“, wie er vom Gerichtshof ausgelegt worden ist, führen.

Änderungsantrag 42

Vorschlag für eine Richtlinie
Erwägung 76

Vorschlag der Kommission	*Geänderter Text*
(76) Um die Wirksamkeit und Abschreckungskraft der Sanktionen bei Verstößen gegen die Verpflichtungen aus dieser Richtlinie zu erhöhen, sollten die zuständigen Behörden befugt sein, Sanktionen zu verhängen, die darin bestehen, die Zertifizierung oder Genehmigung für einen Teil oder alle von einer wesentlichen Einrichtung erbrachten Dienste auszusetzen ***und natürlichen Personen die Ausübung von Leitungsaufgaben vorübergehend zu untersagen***. Angesichts ihrer Schwere und ihrer Auswirkungen auf die Tätigkeiten der	(76) Um die Wirksamkeit und Abschreckungskraft der Sanktionen bei Verstößen gegen die Verpflichtungen aus dieser Richtlinie zu erhöhen, sollten die zuständigen Behörden befugt sein, Sanktionen zu verhängen, die darin bestehen, die Zertifizierung oder Genehmigung für einen Teil ***der*** oder alle von einer wesentlichen Einrichtung erbrachten Dienste auszusetzen. Angesichts ihrer Schwere und ihrer Auswirkungen auf die Tätigkeiten der Einrichtungen und letztlich auf ihre Verbraucher sollten solche Sanktionen im

Einrichtungen und letztlich auf ihre Verbraucher sollten solche Sanktionen im Verhältnis zur Schwere des Verstoßes und unter Berücksichtigung der besonderen Umstände des Einzelfalls verhängt werden; hierzu zählen auch die Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, sowie die zur Verhinderung oder Minderung des erlittenen Schadens und/oder der erlittenen Verluste ergriffenen Maßnahmen. Solche Sanktionen sollten nur als äußerstes Mittel verhängt werden, also erst nachdem die anderen einschlägigen Durchsetzungsmaßnahmen nach dieser Richtlinie ausgeschöpft wurden, und nur so lange, bis die betroffenen Einrichtungen die erforderlichen Maßnahmen zur Behebung der Mängel ergreifen oder die Anforderungen der zuständigen Behörde, auf die sich die Sanktionen beziehen, erfüllen. Für die Verhängung solcher Sanktionen muss es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta der Grundrechte der Europäischen Union, einschließlich des Rechts auf ***wirksamen Rechtsschutz*** und ein faires Verfahren, der Unschuldsvermutung und des Rechts auf Verteidigung, entsprechen.

Verhältnis zur Schwere des Verstoßes und unter Berücksichtigung der besonderen Umstände des Einzelfalls verhängt werden; hierzu zählen auch die Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, sowie die zur Verhinderung oder Minderung des erlittenen Schadens und/oder der erlittenen Verluste ergriffenen Maßnahmen. Solche Sanktionen sollten nur als äußerstes Mittel verhängt werden, also erst nachdem die anderen einschlägigen Durchsetzungsmaßnahmen nach dieser Richtlinie ausgeschöpft wurden, und nur so lange, bis die betroffenen Einrichtungen die erforderlichen Maßnahmen zur Behebung der Mängel ergreifen oder die Anforderungen der zuständigen Behörde, auf die sich die Sanktionen beziehen, erfüllen. Für die Verhängung solcher Sanktionen muss es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta der Grundrechte der Europäischen Union, einschließlich des Rechts auf ***wirksame gerichtliche Rechtsbehelfe*** und ein faires Verfahren, der Unschuldsvermutung und des Rechts auf Verteidigung, entsprechen.

Änderungsantrag 43

Vorschlag für eine Richtlinie
Erwägung 77

Vorschlag der Kommission	*Geänderter Text*
(77) Mit dieser Richtlinie sollten Regeln für die Zusammenarbeit zwischen den zuständigen Behörden und den Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 festgelegt werden, um gegen Verstöße im Zusammenhang mit personenbezogenen Daten vorzugehen.	(77) Mit dieser Richtlinie sollten Regeln für die Zusammenarbeit zwischen den zuständigen Behörden ***gemäß der vorliegenden Richtlinie*** und den Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 festgelegt werden, um gegen Verstöße im Zusammenhang mit personenbezogenen Daten vorzugehen.

Änderungsantrag 44

Vorschlag für eine Richtlinie
Erwägung 79

Vorschlag der Kommission	*Geänderter Text*
(79) Es sollte ein Peer-Review-Mechanismus eingeführt werden, der es ermöglicht, dass von den Mitgliedstaaten benannte Sachverständige die Umsetzung der Cybersicherheitsstrategien, einschließlich der Kapazitäten der Mitgliedstaaten und der verfügbaren Ressourcen, einer Bewertung unterziehen.	(79) Es sollte ein Peer-Review-Mechanismus eingeführt werden, der es ermöglicht, dass von den Mitgliedstaaten benannte Sachverständige die Umsetzung der Cybersicherheitsstrategien, einschließlich der Kapazitäten der Mitgliedstaaten und der verfügbaren Ressourcen, einer Bewertung unterziehen. ***Die EU sollte eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen ermöglichen und Unterstützung anbieten, um zur Erholung nach entsprechenden Cyberangriffen beizutragen.***

Änderungsantrag 45

Vorschlag für eine Richtlinie
Erwägung 82 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(82a) Die vorliegende Richtlinie gilt nicht für die Organe, Einrichtungen und sonstigen Stellen der Union. Allerdings können Einrichtungen der Union als wesentliche oder wichtige Einrichtungen gemäß dieser Richtlinie angesehen werden. Damit durch kohärente und einheitliche Vorschriften ein einheitliches Schutzniveau erreicht wird, sollte die Kommission einen Legislativvorschlag veröffentlichen, um die Organe, Einrichtungen und sonstigen Stellen der Union bis zum 31. Dezember 2022 in den unionsweiten Cybersicherheitsrahmen zu integrieren.

Änderungsantrag 46

Vorschlag für eine Richtlinie
Erwägung 84

Vorschlag der Kommission	*Geänderter Text*
(84) Diese Richtlinie steht mit den in der Charta der Grundrechte der Europäischen Union anerkannten Grundrechten und Grundsätzen, insbesondere der Achtung des Privatlebens und der Kommunikation, dem Schutz personenbezogener Daten, der unternehmerischen Freiheit, dem Eigentumsrecht, dem Recht auf einen wirksamen Rechtsbehelf und dem Recht, gehört zu werden, im Einklang. Diese Richtlinie sollte im Einklang mit diesen Rechten und Grundsätzen umgesetzt werden —	(84) Diese Richtlinie steht mit den in der Charta der Grundrechte der Europäischen Union anerkannten Grundrechten und Grundsätzen, insbesondere der Achtung des Privatlebens und der Kommunikation, dem Schutz personenbezogener Daten, der unternehmerischen Freiheit, dem Eigentumsrecht, dem Recht auf einen wirksamen Rechtsbehelf und dem Recht, gehört zu werden, im Einklang. Diese Richtlinie sollte im Einklang mit diesen Rechten und Grundsätzen ***und unter uneingeschränkter Einhaltung der geltenden Rechtsvorschriften der Union zur Regelung dieser Angelegenheiten*** umgesetzt werden***. Jede Verarbeitung personenbezogener Daten im Rahmen dieser Richtlinie erfolgt im Einklang mit der Verordnung (EU) 2016/679 bzw. der Richtlinie 2002/58/EG entsprechend ihren jeweiligen Anwendungsbereichen, unter anderem im Hinblick auf die Aufgaben und Befugnisse der Aufsichtsbehörden, die für die Überwachung der Einhaltung dieser Rechtsakte zuständig sind —***

Änderungsantrag 47

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Diese Richtlinie gilt für öffentliche und private Einrichtungen der in Anhang I als wesentliche Einrichtungen und in Anhang II als wichtige Einrichtungen aufgeführten Arten. Diese Richtlinie gilt nicht für Einrichtungen, die als Kleinstunternehmen und kleine Unternehmen im Sinne der	(1) Diese Richtlinie gilt für öffentliche und private Einrichtungen der in Anhang I als wesentliche Einrichtungen und in Anhang II als wichtige Einrichtungen aufgeführten Arten. Diese Richtlinie gilt nicht für Einrichtungen, die als Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung

Empfehlung 2003/361/EG der Kommission[28] angesehen werden.	2003/361/EG der Kommission[28] angesehen werden. ***Artikel 3 Absatz 4 des Anhangs der Empfehlung 2003/361/EG der Kommission findet keine Anwendung.***
[28] Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).	[28] Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).

Änderungsantrag 48

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 2 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(2) Unabhängig von der Größe der Einrichtungen gilt diese Richtlinie jedoch auch für die in den Anhängen I und II genannten Einrichtungen, wenn	(2) Unabhängig von der Größe der Einrichtungen gilt diese Richtlinie ***auf der Grundlage einer Risikobewertung nach Artikel 18*** jedoch auch für die in den Anhängen I und II genannten Einrichtungen, wenn

Änderungsantrag 49

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 2 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) es sich bei der Einrichtung um den einzigen Anbieter eines Dienstes ***in einem Mitgliedstaat*** handelt;	c) es sich bei der Einrichtung um den einzigen Anbieter eines Dienstes ***auf nationaler oder regionaler Ebene*** handelt;

Änderungsantrag 50

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 2 – Buchstabe d

Vorschlag der Kommission	*Geänderter Text*
d) sich eine ***mögliche*** Störung des von der Einrichtung erbrachten Dienstes auf die	d) sich eine Störung des von der Einrichtung erbrachten Dienstes auf die

öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken könnte;	öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken könnte;

Änderungsantrag 51

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 2 – Buchstabe e

Vorschlag der Kommission	*Geänderter Text*
e) eine ***mögliche*** Störung des von der Einrichtung erbrachten Dienstes zu Systemrisiken führen könnte, insbesondere in Sektoren, in denen eine solche Störung grenzübergreifende Auswirkungen haben könnte;	e) eine Störung des von der Einrichtung erbrachten Dienstes zu Systemrisiken führen könnte, insbesondere in Sektoren, in denen eine solche Störung grenzübergreifende Auswirkungen haben könnte;

Änderungsantrag 52

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 4 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(4a) Jede Verarbeitung personenbezogener Daten gemäß dieser Richtlinie muss im Einklang mit der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG erfolgen und auf das für die Zwecke dieser Richtlinie unbedingt erforderliche und verhältnismäßige Maß beschränkt sein.

Änderungsantrag 53

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
(5) Unbeschadet des Artikels 346 AEUV werden Informationen, die gemäß den Vorschriften der Union und der Mitgliedstaaten, wie z. B. Vorschriften über das Geschäftsgeheimnis, vertraulich sind, mit der Kommission und anderen zuständigen Behörden nur ausgetauscht,	(5) Unbeschadet des Artikels 346 AEUV werden Informationen, die gemäß den Vorschriften der Union und der Mitgliedstaaten, wie z. B. Vorschriften über das Geschäftsgeheimnis, vertraulich sind, mit der Kommission und anderen zuständigen Behörden nur ausgetauscht,

wenn dieser Austausch für die Anwendung dieser Richtlinie erforderlich ist. Die auszutauschenden Informationen werden auf den zum Zweck dieses Informationsaustauschs ***relevanten und angemessenen*** Umfang beschränkt. Beim Informationsaustausch ***werden*** die Vertraulichkeit der Informationen gewahrt ***sowie*** die Sicherheit und die geschäftlichen Interessen wesentlicher oder wichtiger Einrichtungen geschützt.	wenn dieser Austausch für die Anwendung dieser Richtlinie erforderlich ist. Die auszutauschenden Informationen werden auf den zum Zweck dieses Informationsaustauschs ***notwendigen*** Umfang beschränkt. Beim Informationsaustausch ***wird*** die Vertraulichkeit der Informationen gewahrt***, und*** die Sicherheit und die geschäftlichen Interessen wesentlicher oder wichtiger Einrichtungen ***werden dabei*** geschützt.

Änderungsantrag 54

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 6 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(6a) Damit durch kohärente und einheitliche Vorschriften ein einheitliches Schutzniveau erreicht wird, veröffentlicht die Kommission vor dem 31. Dezember 2021 einen Legislativvorschlag, um die Organe, Einrichtungen und sonstigen Stellen der Union in den allgemeinen unionsweiten Cybersicherheitsrahmen zu integrieren.

Änderungsantrag 55

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 1 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen, oder	b) ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen, ***in das IT-System integriert sind und für die Bereitstellung der Dienste genutzt werden, für die sie vorgesehen sind,*** oder

Änderungsantrag 56

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 4

Vorschlag der Kommission	*Geänderter Text*
4. „nationale Cybersicherheitsstrategie“ einen kohärenten Rahmen eines Mitgliedstaats mit strategischen Zielen und Prioritäten für die ***Sicherheit von Netz- und Informationssystemen*** in diesem Mitgliedstaat;	4. „nationale Cybersicherheitsstrategie“ einen kohärenten Rahmen eines Mitgliedstaats mit strategischen Zielen und Prioritäten für die ***Cybersicherheit*** in diesem Mitgliedstaat;

Änderungsantrag 57

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 12

Vorschlag der Kommission	*Geänderter Text*
12. „Internet-Knoten“ (Internet Exchange Point, IXP) eine Netzeinrichtung, die die Zusammenschaltung von mehr als zwei unabhängigen Netzen (autonomen Systemen) ermöglicht, in erster Linie zur Erleichterung des Austauschs von Internet-Datenverkehr; ein IXP dient nur der Zusammenschaltung autonomer Systeme; ein IXP setzt nicht voraus, dass der Internet-Datenverkehr zwischen zwei beliebigen teilnehmenden autonomen Systemen über ein drittes autonomes System läuft; auch wird der betreffende Datenverkehr weder verändert noch anderweitig beeinträchtigt;	***entfällt***

Änderungsantrag 58

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 22

Vorschlag der Kommission	*Geänderter Text*
22. „Plattform für Dienste sozialer Netzwerke“ eine Plattform, auf der Endnutzer mit unterschiedlichen Geräten	***entfällt***

insbesondere durch Chats, Posts, Videos und Empfehlungen miteinander in Kontakt treten und kommunizieren sowie Inhalte teilen und entdecken können;

Änderungsantrag 59

Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 24

Vorschlag der Kommission	*Geänderter Text*
24. „Einrichtung“ jede natürliche Person oder jede nach dem an ihrem Sitz geltenden nationalen Recht geschaffene und anerkannte juristische Person, die in eigenem Namen Rechte ausüben und Pflichten unterliegen kann;	*(Betrifft nicht die deutsche Fassung.)*

Änderungsantrag 60

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 1 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) eine Beschreibung der für die Cybersicherheitsstrategie des jeweiligen Mitgliedstaats festgelegten Ziele und Prioritäten;	a) eine Beschreibung der für die Cybersicherheitsstrategie des jeweiligen Mitgliedstaats festgelegten Ziele und Prioritäten ***unter Berücksichtigung des allgemeinen Grads des Cybersicherheitsbewusstseins der Bürgerinnen und Bürger sowie des allgemeinen Sicherheitsniveaus bei vernetzten Geräten der Verbraucherinnen und Verbraucher***;

Änderungsantrag 61

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 1 – Buchstabe f

Vorschlag der Kommission	*Geänderter Text*
f) einen politischen Rahmen für eine	f) einen politischen Rahmen für eine

verstärkte Koordinierung zwischen den zuständigen Behörden im Rahmen dieser Richtlinie und der Richtlinie (EU) XXXX/XXXX des Europäischen Parlaments und des Rates [Richtlinie über die Resilienz kritischer Einrichtungen][38] für die Zwecke des Informationsaustauschs über Sicherheitsvorfälle und Cyberbedrohungen und der Wahrnehmung von Aufsichtsaufgaben.

verstärkte Koordinierung zwischen den zuständigen Behörden im Rahmen dieser Richtlinie und der Richtlinie (EU) XXXX/XXXX des Europäischen Parlaments und des Rates [Richtlinie über die Resilienz kritischer Einrichtungen][38]***,*** ***sowohl in als auch zwischen den Mitgliedstaaten,*** für die Zwecke des Informationsaustauschs über Sicherheitsvorfälle und Cyberbedrohungen und der Wahrnehmung von Aufsichtsaufgaben.

---

[38] [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].

[38] [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].

Änderungsantrag 62

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) Leitlinien für die Aufnahme und Spezifikation cybersicherheitsbezogener Anforderungen an IKT-Produkte und -Dienste bei der Vergabe öffentlicher Aufträge;	b) Leitlinien für die Aufnahme und Spezifikation cybersicherheitsbezogener Anforderungen an IKT-Produkte und -Dienste bei der Vergabe öffentlicher Aufträge***, unter anderem einschließlich Verschlüsselungsanforderungen und der Förderung der Verwendung von Open-Source-Cybersicherheitsprodukten***;

Änderungsantrag 63

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe d a (neu)

Vorschlag der Kommission	*Geänderter Text*
	da) ein Konzept in Bezug auf die Aufrechterhaltung der Nutzung offener Daten und von Open-Source-Produkten im Rahmen der Sicherheit durch Transparenz;

Änderungsantrag 64

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe d b (neu)

Vorschlag der Kommission	*Geänderter Text*
	db) ein Konzept zur Förderung des Schutzes und der Sicherheit personenbezogener Daten von Nutzern von Online-Diensten;

Änderungsantrag 65

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe e

Vorschlag der Kommission	*Geänderter Text*
e) ein Konzept zur Förderung und Entwicklung von Cybersicherheitskompetenzen, Sensibilisierungsmaßnahmen sowie Forschungs- und Entwicklungsinitiativen;	e) ein Konzept zur Förderung und Entwicklung von Cybersicherheitskompetenzen, Sensibilisierungsmaßnahmen sowie Forschungs- und Entwicklungsinitiativen***, einschließlich der Entwicklung von Schulungsprogrammen zur Cybersicherheit mit dem Ziel, dafür zu sorgen, dass Einrichtungen Spezialisten und Techniker zur Verfügung stehen***;

Änderungsantrag 66

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe f

Vorschlag der Kommission	*Geänderter Text*
f) ein Konzept zur Unterstützung von Hochschul- und Forschungseinrichtungen ***bei*** der ***Entwicklung von Cybersicherheitsinstrumenten*** und ***sicherer*** Netzinfrastruktur;	f) ein Konzept zur Unterstützung von Hochschul- und Forschungseinrichtungen***, die zu*** der ***nationalen Cybersicherheitsstrategie beitragen, indem sie Cybersicherheitsinstrumente*** und ***eine sichere*** Netzinfrastruktur ***entwickeln und bereitstellen, mit denen zu der nationalen Cybersicherheitsstrategie beigetragen wird, einschließlich spezifischer Konzepte zu Angelegenheiten im Zusammenhang mit der Vertretung und einem ausgewogenen Verhältnis von***

Frauen und Männern in diesem Bereich;

Änderungsantrag 67

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe h

Vorschlag der Kommission	*Geänderter Text*
h) ein Konzept, das auf die spezifischen Bedürfnisse von KMU – insbesondere vom Anwendungsbereich dieser Richtlinie ausgenommener KMU – ausgerichtet ist und Orientierungshilfen sowie Unterstützung bei der Verbesserung ihrer Resilienz gegenüber Cybersicherheitsbedrohungen bietet.	h) ein Konzept, das auf die spezifischen Bedürfnisse von KMU – insbesondere vom Anwendungsbereich dieser Richtlinie ausgenommener KMU – ausgerichtet ist und Orientierungshilfen sowie Unterstützung bei der Verbesserung ihrer Resilienz gegenüber Cybersicherheitsbedrohungen ***und ihrer Fähigkeit zur Reaktion auf Cybersicherheitsvorfälle*** bietet.

Änderungsantrag 68

Vorschlag für eine Richtlinie
Artikel 6 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die ENISA entwickelt und pflegt ein europäisches Schwachstellenregister. Zu diesem Zweck führt die ENISA geeignete Informationssysteme, Konzepte und Verfahren ein und pflegt diese, damit insbesondere wichtige und wesentliche Einrichtungen sowie deren Anbieter von Netz- und Informationssystemen Schwachstellen in IKT-Produkten oder -Diensten offenlegen und registrieren können und allen interessierten Kreisen Zugang zu den im Register enthaltenen Informationen über Schwachstellen gewährt werden kann. Das Register muss insbesondere Folgendes umfassen: Informationen zur Beschreibung der Schwachstelle, des betroffenen IKT-Produkts oder der betroffenen IKT-Dienste sowie zum Ausmaß der Schwachstelle im	(2) Die ENISA entwickelt und pflegt ein europäisches Schwachstellenregister. Zu diesem Zweck führt die ENISA geeignete Informationssysteme, Konzepte und Verfahren ein und pflegt diese, damit insbesondere wichtige und wesentliche Einrichtungen sowie deren Anbieter von Netz- und Informationssystemen Schwachstellen in IKT-Produkten oder -Diensten offenlegen und registrieren können und allen interessierten Kreisen Zugang zu den im Register enthaltenen Informationen über Schwachstellen gewährt werden kann. Das Register muss insbesondere Folgendes umfassen: Informationen zur Beschreibung der Schwachstelle, des betroffenen IKT-Produkts oder der betroffenen IKT-Dienste sowie zum Ausmaß der Schwachstelle im

Hinblick auf die Umstände, unter denen sie ausgenutzt werden kann, Informationen zur Verfügbarkeit entsprechender Patches und bei Nichtverfügbarkeit von Patches Orientierungshilfen für die Nutzer gefährdeter Produkte und Dienste, wie die von offengelegten Schwachstellen ausgehenden Risiken gemindert werden können.	Hinblick auf die Umstände, unter denen sie ausgenutzt werden kann, Informationen zur Verfügbarkeit entsprechender Patches und bei Nichtverfügbarkeit von Patches Orientierungshilfen für die Nutzer gefährdeter Produkte und Dienste, wie die von offengelegten Schwachstellen ausgehenden Risiken gemindert werden können. ***Um dafür zu sorgen, dass die in dem Register enthaltenen Informationen sicher und zugänglich sind, wendet die ENISA dem Stand der Technik entsprechende Sicherheitsmaßnahmen an und stellt die Informationen über entsprechende Schnittstellen in maschinenlesbaren Formaten zur Verfügung.***

Änderungsantrag 69

Vorschlag für eine Richtlinie
Artikel 7 – Absatz 3 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) die Ziele der nationalen ***Vorsorgenmaßnahmen*** und -tätigkeiten;	a) die Ziele der nationalen ***und, soweit zutreffend und anwendbar, regionalen und grenzübergreifenden Vorsorgemaßnahmen*** und -tätigkeiten;

Änderungsantrag 70

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 2 – Buchstabe e

Vorschlag der Kommission	*Geänderter Text*
e) auf Ersuchen einer Einrichtung Durchführung einer ***proaktiven Überprüfung*** der für die Bereitstellung ihrer Dienste verwendeten ***Netz-*** und ***Informationssysteme*** auf ***Schwachstellen (Schwachstellenscan);***	e) auf Ersuchen einer Einrichtung Durchführung einer ***Sicherheitsüberprüfung*** der für die Bereitstellung ihrer Dienste verwendeten ***Informationssysteme*** und ***Netzbereiche, um spezifische Bedrohungen zu erkennen, abzuschwächen oder zu verhindern; die Verarbeitung personenbezogener Daten im***

	Zusammenhang mit einer solchen Überprüfung ist auf das unbedingt erforderliche Maß beschränkt, in jedem Fall jedoch auf IP- und URL-Adressen

Änderungsantrag 71

Vorschlag für eine Richtlinie
Artikel 11 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
(4) Soweit dies zur wirksamen Wahrnehmung der in dieser Richtlinie festgelegten Aufgaben und Pflichten erforderlich ist, sorgen die Mitgliedstaaten für eine angemessene Zusammenarbeit zwischen den zuständigen Behörden und den zentralen Anlaufstellen sowie den Strafverfolgungsbehörden, den Datenschutzbehörden, den gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] für kritische Infrastrukturen zuständigen Behörden und den gemäß der Verordnung (EU) XXXX/XXXX des Europäischen Parlaments und des Rates [DORA-Verordnung][39] in dem jeweiligen Mitgliedstaat benannten nationalen Finanzbehörden.	(4) Soweit dies zur wirksamen Wahrnehmung der in dieser Richtlinie festgelegten Aufgaben und Pflichten erforderlich ist, sorgen die Mitgliedstaaten für eine angemessene Zusammenarbeit zwischen den zuständigen Behörden und den zentralen Anlaufstellen sowie den Strafverfolgungsbehörden, den Datenschutzbehörden, den gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] für kritische Infrastrukturen zuständigen Behörden und den gemäß der Verordnung (EU) XXXX/XXXX des Europäischen Parlaments und des Rates [DORA-Verordnung][39] in dem jeweiligen Mitgliedstaat benannten nationalen Finanzbehörden ***im Einklang mit ihren jeweiligen Zuständigkeiten***.
[39] [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].	[39] [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].

Änderungsantrag 72

Vorschlag für eine Richtlinie
Artikel 11 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
(5) Die Mitgliedstaaten stellen sicher, dass ihre zuständigen Behörden die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer	(5) Die Mitgliedstaaten stellen sicher, dass ihre zuständigen Behörden die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer

Einrichtungen] benannten zuständigen Behörden regelmäßig über Cybersicherheitsrisiken, Cyberbedrohungen und Sicherheitsvorfälle unterrichten, die als kritische Einrichtungen oder kritischen Einrichtungen gleichgestellte Einrichtungen gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] ermittelte wesentliche Einrichtungen betreffen, sowie über die von den zuständigen Behörden als Reaktion auf diese Risiken und Sicherheitsvorfälle ergriffenen Maßnahmen.	Einrichtungen] benannten zuständigen Behörden regelmäßig ***und rechtzeitig*** über Cybersicherheitsrisiken, Cyberbedrohungen und Sicherheitsvorfälle unterrichten, die als kritische Einrichtungen oder kritischen Einrichtungen gleichgestellte Einrichtungen gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] ermittelte wesentliche Einrichtungen betreffen, sowie über die von den zuständigen Behörden als Reaktion auf diese Risiken und Sicherheitsvorfälle ergriffenen Maßnahmen.

Änderungsantrag 73

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 3 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(3) Die Kooperationsgruppe setzt sich aus Vertretern der Mitgliedstaaten, der Kommission und der ENISA zusammen. Der Europäische Auswärtige Dienst ***nimmt*** an den Tätigkeiten der Kooperationsgruppe als Beobachter teil. Die Europäischen Aufsichtsbehörden (ESAs) können sich gemäß Artikel 17 Absatz 5 Buchstabe c der Verordnung (EU) XXXX/XXXX [DORA-Verordnung] an den Tätigkeiten der Kooperationsgruppe beteiligen.	(3) Die Kooperationsgruppe setzt sich aus Vertretern der Mitgliedstaaten, der Kommission und der ENISA zusammen. Der Europäische Auswärtige Dienst***, das Europäische Zentrum zur Bekämpfung der Cyberkriminalität bei Europol und der Europäische Datenschutzausschuss nehmen*** an den Tätigkeiten der Kooperationsgruppe als Beobachter teil. Die Europäischen Aufsichtsbehörden (ESAs) können sich gemäß Artikel 17 Absatz 5 Buchstabe c der Verordnung (EU) XXXX/XXXX [DORA-Verordnung] an den Tätigkeiten der Kooperationsgruppe beteiligen.

Änderungsantrag 74

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 3 – Unterabsatz 1

Vorschlag der Kommission	*Geänderter Text*
Gegebenenfalls kann die Kooperationsgruppe Vertreter der maßgeblichen Interessenträger ***einladen,*** an ihren Arbeiten ***teilzunehmen***.	***Wenn dies für die Erfüllung ihrer Aufgaben von Bedeutung ist, lädt*** die Kooperationsgruppe Vertreter der maßgeblichen Interessenträger ***zur Teilnahme*** an ihren Arbeiten ***und das Europäische Parlament zur Teilnahme als Beobachter ein***.

Änderungsantrag 75

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 8

Vorschlag der Kommission	*Geänderter Text*
(8) Die Kooperationsgruppe tagt regelmäßig, mindestens aber ***einmal*** jährlich gemeinsam mit der mit der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] eingerichteten Gruppe für die Resilienz kritischer Einrichtungen, um die strategische Zusammenarbeit und den Informationsaustausch zu ***fördern***.	(8) Die Kooperationsgruppe tagt regelmäßig, mindestens aber ***zweimal*** jährlich gemeinsam mit der mit der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] eingerichteten Gruppe für die Resilienz kritischer Einrichtungen, um die strategische Zusammenarbeit und den Informationsaustausch ***in Echtzeit*** zu ***erleichtern***.

Änderungsantrag 76

Vorschlag für eine Richtlinie
Artikel 13 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Das CSIRT-Netzwerk setzt sich aus Vertretern der CSIRTs der Mitgliedstaaten und des CERT-EU zusammen. Die Kommission ***nimmt*** als ***Beobachterin*** am CSIRT-Netzwerk teil. Die ENISA führt die Sekretariatsgeschäfte und unterstützt aktiv die Zusammenarbeit zwischen den CSIRTs.	(2) Das CSIRT-Netzwerk setzt sich aus Vertretern der CSIRTs der Mitgliedstaaten und des CERT-EU zusammen. Die Kommission ***und das Europäische Zentrum zur Bekämpfung der Cyberkriminalität bei Europol nehmen*** als ***Beobachter*** am CSIRT-Netzwerk teil. Die ENISA führt die Sekretariatsgeschäfte und unterstützt aktiv die Zusammenarbeit zwischen den CSIRTs.

Änderungsantrag 77

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) EU-CyCLONe setzt sich aus den Vertretern der gemäß Artikel 7 benannten für das Krisenmanagement zuständigen Behörden der Mitgliedstaaten, der Kommission und der ENISA zusammen. ENISA führt die Sekretariatsgeschäfte des Netzwerks und unterstützt den sicheren Informationsaustausch.	(2) EU-CyCLONe setzt sich aus den Vertretern der gemäß Artikel 7 benannten für das Krisenmanagement zuständigen Behörden der Mitgliedstaaten, der Kommission und der ENISA zusammen. ***Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität bei Europol nimmt als Beobachter an den Tätigkeiten von EU-CyCLONe teil.*** ENISA führt die Sekretariatsgeschäfte des Netzwerks und unterstützt den sicheren Informationsaustausch.

Änderungsantrag 78

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
(6) EU-CyCLONe arbeitet auf der Grundlage vereinbarter Verfahrensmodalitäten mit dem CSIRT-Netzwerk zusammen.	(6) EU-CyCLONe arbeitet auf der Grundlage vereinbarter Verfahrensmodalitäten mit dem CSIRT-Netzwerk ***und mit Strafverfolgungsbehörden im Rahmen des Notfallprotokolls der EU für die Reaktion der Strafverfolgungsbehörden*** zusammen.

Änderungsantrag 79

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 1 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(1) Die ENISA veröffentlicht in Zusammenarbeit mit der Kommission einen ***zweijährlichen Bericht*** über den Stand der Cybersicherheit in der Union. Dieser Bericht muss insbesondere Folgendes enthalten:	(1) Die ENISA veröffentlicht in Zusammenarbeit mit der Kommission einen ***Jahresbericht*** über den Stand der Cybersicherheit in der Union. Dieser Bericht muss ***in einem maschinenlesbaren Format erstellt werden und*** insbesondere

Folgendes enthalten:

Änderungsantrag 80

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 1 – Buchstabe c a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ca) die Auswirkungen von Cybersicherheitsvorfällen auf den Schutz personenbezogener Daten in der Union.

Änderungsantrag 81

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 1 – Buchstabe c b (neu)

Vorschlag der Kommission	*Geänderter Text*
	cb) einen Überblick über den allgemeinen Grad der Sensibilisierung der Bürger für das Thema Cybersicherheit und das entsprechende Verhalten der Bürger sowie über das allgemeine Sicherheitsniveau verbraucherorientierter vernetzter Geräte, die in der Union in Verkehr gebracht werden.

Änderungsantrag 82

Vorschlag für eine Richtlinie
Artikel 17 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Mitgliedstaaten stellen sicher, dass die Mitglieder der Leitungsorgane regelmäßig an spezifischen Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf den Betrieb der Einrichtung zu	(2) Die Mitgliedstaaten stellen sicher, dass die Mitglieder der Leitungsorgane ***und die zuständigen Sachverständigen für Cybersicherheit*** regelmäßig an spezifischen Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von ***sich wandelnden*** Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen

erwerben.	auf den Betrieb der Einrichtung zu erwerben.

Änderungsantrag 83

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die ***Sicherheit*** der Netz- und Informationssysteme, die ***diese Einrichtungen bei der*** Erbringung ihrer Dienste ***nutzen***, zu beherrschen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein ***Sicherheitsniveau*** der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist.	(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um ***mit Blick auf*** die ***Sicherstellung der Kontinuität dieser Dienste und die Minderung der*** Risiken für die ***Rechte von Einzelpersonen bei der Verarbeitung ihrer personenbezogenen Daten die Risiken für die Cybersicherheit*** der Netz- und Informationssysteme, die ***für die*** Erbringung ihrer Dienste ***genutzt werden***, zu beherrschen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein ***Cybersicherheitsniveau*** der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist.

Änderungsantrag 84

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 2 – Buchstabe g

Vorschlag der Kommission	*Geänderter Text*
g) Einsatz von Kryptografie und Verschlüsselung.	g) Einsatz von Kryptografie und ***einer starken*** Verschlüsselung.

Änderungsantrag 85

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Die Mitgliedstaaten stellen sicher, dass die Einrichtungen bei der Erwägung geeigneter Maßnahmen nach Absatz 2 Buchstabe d die spezifischen Schwachstellen der einzelnen Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, berücksichtigen.	(3) Die Mitgliedstaaten stellen sicher, dass die Einrichtungen bei der Erwägung geeigneter ***und verhältnismäßiger*** Maßnahmen nach Absatz 2 Buchstabe d die spezifischen Schwachstellen der einzelnen Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, berücksichtigen. ***Die zuständigen Behörden stellen den Einrichtungen Orientierungshilfen für die praktische und verhältnismäßige Anwendung zur Verfügung.***

Änderungsantrag 86

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 6 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(6a) Die Mitgliedstaaten räumen dem Nutzer eines von einer wesentlichen oder wichtigen Einrichtung bereitgestellten Netz- und Informationssystems das Recht ein, von der Einrichtung Informationen über die technischen und organisatorischen Maßnahmen zu erhalten, die getroffen wurden, um die Risiken für die Sicherheit von Netz- und Informationssystemen zu bewältigen. Die Mitgliedstaaten legen die Beschränkungen für dieses Recht fest.

Änderungsantrag 87

Vorschlag für eine Richtlinie
Artikel 19 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Die Kooperationsgruppe ***kann*** in Zusammenarbeit mit der Kommission und der ENISA koordinierte	(1) Die Kooperationsgruppe ***führt*** in Zusammenarbeit mit der Kommission und der ENISA koordinierte

Risikobewertungen in Bezug auf die Sicherheit der Lieferketten bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte unter Berücksichtigung technischer und erforderlichenfalls nichttechnischer Risikofaktoren ***durchführen***.	Risikobewertungen in Bezug auf die Sicherheit der Lieferketten bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte unter Berücksichtigung technischer und erforderlichenfalls nichttechnischer Risikofaktoren ***durch***.

Änderungsantrag 88

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen den zuständigen Behörden oder dem CSIRT gemäß den Absätzen 3 und 4 unverzüglich jeden Sicherheitsvorfall melden, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste hat***. Gegebenenfalls unterrichten*** diese Einrichtungen die Empfänger ihrer Dienste unverzüglich über Sicherheitsvorfälle, die die Erbringung des jeweiligen Dienstes beeinträchtigen könnten. Die Mitgliedstaaten stellen sicher, dass diese Einrichtungen unter anderem alle Informationen übermitteln, die es den zuständigen Behörden oder dem CSIRT ermöglichen zu ermitteln, ob der Sicherheitsvorfall grenzübergreifende Auswirkungen hat.	(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen den zuständigen Behörden oder dem CSIRT gemäß den Absätzen 3 und 4 unverzüglich***, in jedem Fall aber innerhalb von 24 Stunden,*** jeden Sicherheitsvorfall melden, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste hat***, sowie den zuständigen Strafverfolgungsbehörden, wenn der Vorfall mutmaßlich oder bekanntermaßen böswilliger Natur ist.*** Diese Einrichtungen ***unterrichten*** die Empfänger ihrer Dienste unverzüglich***, in jedem Fall aber innerhalb von 24 Stunden,*** über Sicherheitsvorfälle, die die Erbringung des jeweiligen Dienstes beeinträchtigen könnten***, und stellen Informationen bereit, die es ihnen ermöglichen würden, die nachteiligen Auswirkungen der Cyberangriffe abzumildern. In Ausnahmefällen, wenn die Offenlegung weitere Cyberangriffe auslösen könnte, können diese Einrichtungen die Unterrichtung verzögern***. Die Mitgliedstaaten stellen sicher, dass diese Einrichtungen unter anderem alle Informationen übermitteln, die es den zuständigen Behörden oder dem CSIRT ermöglichen zu ermitteln, ob der Sicherheitsvorfall grenzübergreifende Auswirkungen hat.

Änderungsantrag 89

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 2 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(2) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen den zuständigen Behörden oder dem CSIRT ***unverzüglich*** jede von diesen Einrichtungen ermittelte erhebliche Cyberbedrohung melden, die nach deren Auffassung möglicherweise zu einem erheblichen Sicherheitsvorfall hätte führen können.	(2) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen ***in der Lage sind,*** den zuständigen Behörden oder dem CSIRT jede von diesen Einrichtungen ermittelte erhebliche Cyberbedrohung ***zu*** melden, die nach deren Auffassung möglicherweise zu einem erheblichen Sicherheitsvorfall hätte führen können.

Änderungsantrag 90

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 2 – Unterabsatz 1

Vorschlag der Kommission	*Geänderter Text*
Gegebenenfalls ***unterrichten*** diese Einrichtungen die potenziell von einer erheblichen Cyberbedrohung betroffenen Empfänger ihrer Dienste ***unverzüglich*** über alle Maßnahmen oder Abhilfemaßnahmen, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. ***Die Einrichtungen*** informieren diese Empfänger ***gegebenenfalls*** auch über die Bedrohung selbst. Mit der Meldung wird keine höhere Haftung der meldenden Einrichtung begründet.	Gegebenenfalls ***erhalten*** diese Einrichtungen ***die Möglichkeit,*** die potenziell von einer erheblichen Cyberbedrohung betroffenen Empfänger ihrer Dienste über alle Maßnahmen oder Abhilfemaßnahmen ***zu unterrichten***, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. ***Wenn eine derartige Meldung erfolgt,*** informieren ***die Einrichtungen*** diese Empfänger auch über die Bedrohung selbst. Mit der Meldung wird keine höhere Haftung der meldenden Einrichtung begründet.

Änderungsantrag 91

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Buchstabe c – Einleitung

Vorschlag der Kommission	*Geänderter Text*
c) spätestens einen Monat nach Vorlage des Berichts gemäß Buchstabe a einen ***Abschlussbericht***, der mindestens Folgendes enthält:	c) spätestens einen Monat nach Vorlage des Berichts gemäß Buchstabe a einen ***umfassenden Bericht***, der mindestens Folgendes enthält:

Änderungsantrag 92

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Buchstabe c – Ziffer ii

Vorschlag der Kommission	*Geänderter Text*
ii) Angaben zur Art der ***Bedrohung*** bzw. zugrunde liegenden Ursache, die den Sicherheitsvorfall wahrscheinlich ausgelöst hat;	ii) Angaben zur Art der ***Cyberbedrohung*** bzw. zugrunde liegenden Ursache, die den Sicherheitsvorfall wahrscheinlich ausgelöst hat;

Änderungsantrag 93

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Buchstabe c – Ziffer iii

Vorschlag der Kommission	*Geänderter Text*
iii) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen.	iii) Angaben zu den getroffenen und laufenden ***Minderungs- oder*** Abhilfemaßnahmen.

Änderungsantrag 94

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
(6) Gegebenenfalls und insbesondere, wenn der in Absatz 1 genannte Sicherheitsvorfall zwei oder mehr Mitgliedstaaten betrifft, unterrichtet die zuständige Behörde oder das CSIRT, der bzw. dem die Meldung erstattet wurde, die anderen betroffenen Mitgliedstaaten und die ENISA über den Sicherheitsvorfall.	(6) Gegebenenfalls und insbesondere, wenn der in Absatz 1 genannte Sicherheitsvorfall zwei oder mehr Mitgliedstaaten betrifft, unterrichtet die zuständige Behörde oder das CSIRT, der bzw. dem die Meldung erstattet wurde, die anderen betroffenen Mitgliedstaaten und die ENISA über den Sicherheitsvorfall.

Dabei wahren die zuständigen Behörden, die CSIRTs und die zentralen Anlaufstellen im Einklang mit dem Unionsrecht oder mit den dem Unionsrecht entsprechenden nationalen Rechtsvorschriften die Sicherheit und das wirtschaftliche Interesse der Einrichtung sowie die Vertraulichkeit der bereitgestellten Informationen.	***Wenn der Vorfall zwei oder mehr Mitgliedstaaten betrifft und mutmaßlichen kriminellen Hintergrund hat, unterrichtet die zuständige Behörde oder das CSIRT EUROPOL.*** Dabei wahren die zuständigen Behörden, die CSIRTs und die zentralen Anlaufstellen im Einklang mit dem Unionsrecht oder mit den dem Unionsrecht entsprechenden nationalen Rechtsvorschriften die Sicherheit und das wirtschaftliche Interesse der Einrichtung sowie die Vertraulichkeit der bereitgestellten Informationen.

Änderungsantrag 95

Vorschlag für eine Richtlinie
Artikel 22 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) ***In*** Zusammenarbeit mit den Mitgliedstaaten bietet die ENISA Beratung und erlässt Leitlinien zu den technischen Bereichen, die in Bezug auf Absatz 1 in Betracht zu ziehen sind, sowie zu den bereits bestehenden Normen — einschließlich der nationalen Normen der Mitgliedstaaten —, mit denen diese Bereiche abgedeckt werden könnten.	(2) ***Nach Abstimmung mit dem EDSA und in*** Zusammenarbeit mit den Mitgliedstaaten bietet die ENISA Beratung und erlässt Leitlinien zu den technischen Bereichen, die in Bezug auf Absatz 1 in Betracht zu ziehen sind, sowie zu den bereits bestehenden Normen – einschließlich der nationalen Normen der Mitgliedstaaten –, mit denen diese Bereiche abgedeckt werden könnten.

Änderungsantrag 96

Vorschlag für eine Richtlinie
Artikel 23 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domänennamensystems zu leisten, stellen die Mitgliedstaaten sicher, dass die ***TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen***, genaue und	(1) Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domänennamensystems zu leisten, stellen die Mitgliedstaaten sicher, dass die ***TLD über Vorgaben und Verfahren verfügen, mit denen sichergestellt wird***, ***dass*** genaue und vollständige Domänennamen-

vollständige Domänennamen-Registrierungsdaten in einer eigenen Datenbank ***sammeln und pflegen, wobei die*** Datenschutzvorschriften der Union in Bezug auf personenbezogene Daten ***mit der gebotenen Sorgfalt zu beachten sind***.	Registrierungsdaten in einer eigenen Datenbank ***im Einklang mit den*** Datenschutzvorschriften der Union in Bezug auf personenbezogene Daten ***gesammelt und gepflegt werden. Die Mitgliedstaaten stellen sicher, dass diese Vorgaben und Verfahren öffentlich zugänglich gemacht werden.***

Änderungsantrag 97

Vorschlag für eine Richtlinie
Artikel 23 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Mitgliedstaaten stellen sicher, dass die Datenbanken zu den in Absatz 1 genannten Domänennamen-Registrierungsdaten ***einschlägige*** Angaben enthalten, anhand derer die Inhaber der Domänennamen und die Kontaktstellen, die die Domänennamen im Rahmen der TLD verwalten, identifiziert und kontaktiert werden können.	(2) Die Mitgliedstaaten stellen sicher, dass die Datenbanken zu den in Absatz 1 genannten Domänennamen-Registrierungsdaten ***die erforderlichen*** Angaben***, nämlich Name, Anschrift, E-Mail-Adresse und Telefonnummer,*** enthalten, anhand derer die Inhaber der Domänennamen und die Kontaktstellen, die die Domänennamen im Rahmen der TLD verwalten, identifiziert und kontaktiert werden können.

Änderungsantrag 98

Vorschlag für eine Richtlinie
Artikel 23 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, über Vorgaben und Verfahren verfügen, mit denen sichergestellt wird, dass die Datenbanken genaue und vollständige Angaben enthalten. Die Mitgliedstaaten stellen sicher, dass diese Vorgaben und Verfahren öffentlich zugänglich gemacht werden.	***entfällt***

Begründung

Dieser Absatz wurde in Artikel 23 Absatz 1 eingefügt.

Änderungsantrag 99

Vorschlag für eine Richtlinie
Artikel 23 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
(4) Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, unverzüglich nach der Registrierung eines Domänennamens ***die nicht personenbezogenen Domänenregistrierungsdaten*** veröffentlichen.	(4) Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, ***gemäß Artikel 6 Absatz 1 Buchstabe c und Artikel 6 Absatz 3 der Verordnung (EU) 2016/679*** unverzüglich nach der Registrierung eines Domänennamens ***bestimmte Domänennamen-Registrierungsdaten*** veröffentlichen***, etwa den Domänennamen und den Namen der juristischen Person***.

Änderungsantrag 100

Vorschlag für eine Richtlinie
Artikel 23 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
(5) Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, auf rechtmäßige und hinreichend begründete Anträge ***berechtigten Zugangsnachfragern*** im Einklang mit dem Datenschutzrecht der Union Zugang zu bestimmten Domänennamen-Registrierungsdaten gewähren. Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, alle Anträge auf Zugang	(5) Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, auf rechtmäßige und hinreichend begründete Anträge ***von Behörden, einschließlich zuständiger Behörden gemäß dieser Richtlinie, Behörden, die nach Unionsrecht oder nationalem Recht für die Verhütung, Ermittlung oder Verfolgung von Straftaten zuständig sind, oder Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679,*** im Einklang mit dem Datenschutzrecht der Union

unverzüglich beantworten. Die Mitgliedstaaten stellen sicher, dass die Vorgaben und Verfahren für die Offenlegung solcher Daten öffentlich zugänglich gemacht werden.

Zugang zu bestimmten Domänennamen-Registrierungsdaten gewähren. Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, alle ***rechtmäßigen und hinreichend begründeten*** Anträge auf Zugang unverzüglich beantworten. Die Mitgliedstaaten stellen sicher, dass die Vorgaben und Verfahren für die Offenlegung solcher Daten öffentlich zugänglich gemacht werden.

Änderungsantrag 101

Vorschlag für eine Richtlinie
Artikel 24 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Hat eine in Absatz 1 genannte Einrichtung keine Niederlassung in der Union, bietet aber Dienstleistungen innerhalb der Union an, muss sie einen Vertreter in der Union benennen. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die Dienste angeboten werden. ***Es*** gilt, dass solche Einrichtungen der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegen, in dem der Vertreter niedergelassen ist. Wurde in der Union kein Vertreter im Sinne dieses Artikels benannt, kann jeder Mitgliedstaat, in dem die Einrichtung Dienste erbringt, gegen die Einrichtung rechtliche Schritte wegen Nichteinhaltung der Verpflichtungen nach dieser Richtlinie einleiten.	(3) Hat eine in Absatz 1 genannte Einrichtung keine Niederlassung in der Union, bietet aber Dienstleistungen innerhalb der Union an, muss sie einen Vertreter in der Union benennen. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die Dienste angeboten werden. ***Unbeschadet der Zuständigkeiten der Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679*** gilt, dass solche Einrichtungen der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegen, in dem der Vertreter niedergelassen ist. Wurde in der Union kein Vertreter im Sinne dieses Artikels benannt, kann jeder Mitgliedstaat, in dem die Einrichtung Dienste erbringt, gegen die Einrichtung rechtliche Schritte wegen Nichteinhaltung der Verpflichtungen nach dieser Richtlinie einleiten.

Änderungsantrag 102

Vorschlag für eine Richtlinie
Artikel 25 – Absatz 1 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(1) Die ENISA erstellt und pflegt ein Register wesentlicher und wichtiger Einrichtungen im Sinne des Artikels 24 Absatz 1. Die Einrichtungen übermitteln der ENISA spätestens bis zum … [12 Monate nach Inkrafttreten der Richtlinie] folgende Angaben:	(1) Die ENISA erstellt und pflegt ein ***sicheres*** Register wesentlicher und wichtiger Einrichtungen im Sinne des Artikels 24 Absatz 1. Die Einrichtungen übermitteln der ENISA spätestens bis zum … [12 Monate nach Inkrafttreten der Richtlinie] folgende Angaben:

Änderungsantrag 103

Vorschlag für eine Richtlinie
Artikel 26 – Absatz 1 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(1) Unbeschadet der Verordnung (EU) 2016/679 stellen die Mitgliedstaaten sicher, dass wesentliche und wichtige Einrichtungen relevante Cybersicherheitsinformationen untereinander austauschen können, einschließlich Informationen über Cyberbedrohungen, Schwachstellen, Gefährdungsindikatoren (indicators of compromise – IoC), Taktiken, Techniken und Verfahren, Cybersicherheitswarnungen und Konfigurationstools, sofern	(1) Unbeschadet der Verordnung (EU) 2016/679 ***oder der Richtlinie 2002/58/EG*** stellen die Mitgliedstaaten sicher, dass wesentliche und wichtige Einrichtungen relevante Cybersicherheitsinformationen untereinander austauschen können, einschließlich Informationen über Cyberbedrohungen, Schwachstellen, Gefährdungsindikatoren (indicators of compromise – IoC), Taktiken, Techniken und Verfahren, Cybersicherheitswarnungen und Konfigurationstools ***sowie den Aufenthaltsort oder die Identität des Angreifers***, sofern

Änderungsantrag 104

Vorschlag für eine Richtlinie
Artikel 28 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) ***Bei*** der Bearbeitung von Sicherheitsvorfällen, die zur Verletzung des Schutzes personenbezogener Daten führen, ***arbeiten die zuständigen Behörden*** eng mit den ***Datenschutzbehörden*** zusammen.	(2) ***Unbeschadet der Zuständigkeiten, Aufgaben und Befugnisse der Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 arbeiten die zuständigen Behörden bei*** der Bearbeitung von Sicherheitsvorfällen, die zur Verletzung des Schutzes

	personenbezogener Daten führen, eng mit den ***Aufsichtsbehörden*** zusammen. ***Zu diesem Zweck tauschen die zuständigen Behörden und Aufsichtsbehörden Informationen aus, die für ihren jeweiligen Zuständigkeitsbereich relevant sind. Darüber hinaus stellen die zuständigen Behörden den zuständigen Aufsichtsbehörden auf Verlangen alle Informationen zur Verfügung, die sie im Rahmen von Prüfungen und Untersuchungen im Zusammenhang mit der Verarbeitung personenbezogener Daten erhalten haben.***

Änderungsantrag 105

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 4 – Buchstabe h

Vorschlag der Kommission	*Geänderter Text*
h) diese Einrichtungen anzuweisen, Aspekte der Nichteinhaltung der in dieser Richtlinie festgelegten Verpflichtungen entsprechend bestimmter Vorgaben öffentlich bekannt zu machen;	***entfällt***

Änderungsantrag 106

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 5 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) gegen Personen, die auf Geschäftsführungs- bzw. Vorstandsebene oder Ebene des rechtlichen Vertreters Leitungsaufgaben in dieser wesentlichen Einrichtung wahrnehmen, und gegen jede andere natürliche Person, die für den Verstoß Verantwortung trägt, ein vorübergehendes Verbot zur Wahrnehmung von Leitungsaufgaben in dieser Einrichtung zu verhängen oder von den zuständigen Stellen oder Gerichten die Verhängung eines solchen Verbots zu	***entfällt***

verlangen.

Änderungsantrag 107

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 5 – Unterabsatz 1

Vorschlag der Kommission	*Geänderter Text*
Diese ***Sanktionen werden*** nur so lange angewandt, bis die Einrichtung die erforderlichen Maßnahmen ergreift, um die Mängel zu beheben oder die Anforderungen der zuständigen Behörde, wegen deren Nichterfüllung die Sanktionen verhängt wurden, zu erfüllen.	Diese ***Sanktion wird*** nur so lange angewandt, bis die Einrichtung die erforderlichen Maßnahmen ergreift, um die Mängel zu beheben oder die Anforderungen der zuständigen Behörde, wegen deren Nichterfüllung die Sanktionen verhängt wurden, zu erfüllen.

Änderungsantrag 108

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 7 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) die Höhe des tatsächlich entstandenen Schadens bzw. entstandener Verluste ***oder potenzieller Schäden oder Verluste, die hätten verursacht werden können***, sofern sich diese feststellen lassen. Bei der Bewertung dieses Aspekts sind unter anderem tatsächliche oder potenzielle finanzielle oder wirtschaftliche Verluste, Auswirkungen auf andere Dienste sowie die Zahl der betroffenen oder potenziell betroffenen Nutzer zu berücksichtigen;	c) die Höhe des tatsächlich entstandenen ***materiellen oder immateriellen*** Schadens bzw. entstandener Verluste, sofern sich diese feststellen lassen. Bei der Bewertung dieses Aspekts sind unter anderem tatsächliche oder potenzielle finanzielle oder wirtschaftliche Verluste, Auswirkungen auf andere Dienste sowie die Zahl der betroffenen oder potenziell betroffenen Nutzer zu berücksichtigen;

Änderungsantrag 109

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 7 – Buchstabe c a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ca) alle einschlägigen früheren

Verstöße der betroffenen Einrichtung;

Änderungsantrag 110

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 7 – Buchstabe c b (neu)

Vorschlag der Kommission	*Geänderter Text*
	cb) die Art und Weise, wie der Verstoß der zuständigen Behörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang die Einrichtung den Verstoß gemeldet hat;

Änderungsantrag 111

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 7 – Buchstabe g

Vorschlag der Kommission	*Geänderter Text*
g) Umfang der Zusammenarbeit ***der verantwortlichen natürlichen oder juristischen Person(en)*** mit den zuständigen Behörden***.***	g) Umfang der Zusammenarbeit mit den zuständigen Behörden***, um dem Verstoß abzuhelfen und mögliche nachteilige Auswirkungen der Verstöße zu mindern;***

Änderungsantrag 112

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 7 – Buchstabe g a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ga) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

Änderungsantrag 113

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 9

Vorschlag der Kommission	*Geänderter Text*
(9) Die Mitgliedstaaten stellen sicher, dass ihre zuständigen Behörden bei der Ausübung ihrer Aufsichts- und Durchsetzungsbefugnisse, mit denen sichergestellt werden soll, dass wesentliche Einrichtungen, die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] als kritische Einrichtungen oder als einer kritischen Einrichtung gleichgestellte Einrichtungen eingestuft wurden, die Verpflichtungen aus dieser Richtlinie erfüllen, die jeweils zuständigen Behörden ***des betreffenden Mitgliedstaats***, die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannt wurden, unterrichten. Auf Ersuchen von gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] zuständigen Behörden dürfen die zuständigen Behörden ihre Aufsichts- und Durchsetzungsbefugnisse in Bezug auf eine als kritisch oder als einer kritischen Einrichtung gleichwertig eingestufte wesentliche Einrichtung ausüben.	(9) Die Mitgliedstaaten stellen sicher, dass ihre zuständigen Behörden bei der Ausübung ihrer Aufsichts- und Durchsetzungsbefugnisse, mit denen sichergestellt werden soll, dass wesentliche Einrichtungen, die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] als kritische Einrichtungen oder als einer kritischen Einrichtung gleichgestellte Einrichtungen eingestuft wurden, die Verpflichtungen aus dieser Richtlinie erfüllen, die jeweils zuständigen Behörden ***aller Mitgliedstaaten***, die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannt wurden, ***in Echtzeit*** unterrichten. Auf Ersuchen von gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] zuständigen Behörden dürfen die zuständigen Behörden ihre Aufsichts- und Durchsetzungsbefugnisse in Bezug auf eine als kritisch oder als einer kritischen Einrichtung gleichwertig eingestufte wesentliche Einrichtung ausüben.

Änderungsantrag 114

Vorschlag für eine Richtlinie
Artikel 30 – Absatz 4 – Buchstabe g

Vorschlag der Kommission	*Geänderter Text*
g) diese Einrichtungen anzuweisen, Aspekte der Nichteinhaltung ihrer in dieser Richtlinie festgelegten Verpflichtungen entsprechend bestimmter Vorgaben öffentlich bekannt zu machen;	***entfällt***

Änderungsantrag 115

Vorschlag für eine Richtlinie
Artikel 30 – Absatz 4 – Buchstabe h

Vorschlag der Kommission	*Geänderter Text*
h) eine öffentliche Erklärung abzugeben, in der die Art des Verstoßes sowie die juristische(n) ***und natürliche(n)*** Person(en) genannt wird bzw. werden, die für den Verstoß gegen eine in dieser Richtlinie festgelegte Verpflichtung verantwortlich ist bzw. sind;	h) eine öffentliche Erklärung abzugeben, in der die Art des Verstoßes sowie die juristische(n) Person(en) genannt wird bzw. werden, die für den Verstoß gegen eine in dieser Richtlinie festgelegte Verpflichtung verantwortlich ist bzw. sind;

Änderungsantrag 116

Vorschlag für eine Richtlinie
Artikel 31 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Geldbußen werden ***je nach den Umständen des Einzelfalls*** zusätzlich zu oder anstelle von Maßnahmen nach Artikel 29 Absatz 4 Buchstaben a bis i, Artikel 29 Absatz 5 und Artikel 30 Absatz 4 Buchstaben a bis h verhängt.	(2) Geldbußen werden zusätzlich zu oder anstelle von Maßnahmen nach Artikel 29 Absatz 4 Buchstaben a bis i, Artikel 29 Absatz 5 und Artikel 30 Absatz 4 Buchstaben a bis h verhängt***, je nach den Umständen des Einzelfalls***.

Änderungsantrag 117

Vorschlag für eine Richtlinie
Artikel 31 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) ***Bei der Entscheidung über die Verhängung einer*** Geldbuße und deren Höhe sind in jedem Einzelfall zumindest die in Artikel 29 Absatz 7 genannten Elemente gebührend zu berücksichtigen.	(3) ***Ob eine*** Geldbuße ***verhängt wird, hängt von den Umständen des Einzelfalls ab,*** und ***bei der Entscheidung über*** deren Höhe sind in jedem Einzelfall zumindest die in Artikel 29 Absatz 7 genannten Elemente gebührend zu berücksichtigen.

Änderungsantrag 118

Vorschlag für eine Richtlinie
Artikel 32 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Haben die zuständigen Behörden Hinweise darauf, dass der Verstoß einer wesentlichen oder wichtigen Einrichtung gegen die in den Artikeln 18 und 20 festgelegten Verpflichtungen eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Absatz 12 der Verordnung (EU) 2016/679 zur Folge hat, die gemäß Artikel 33 der genannten Verordnung zu melden ist, unterrichten sie die gemäß den Artikeln 55 und 56 jener Verordnung zuständigen Aufsichtsbehörden ***innerhalb einer angemessenen Frist***.	(1) Haben die zuständigen Behörden Hinweise darauf, dass der Verstoß einer wesentlichen oder wichtigen Einrichtung gegen die in den Artikeln 18 und 20 festgelegten Verpflichtungen eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Absatz 12 der Verordnung (EU) 2016/679 zur Folge hat, die gemäß Artikel 33 der genannten Verordnung zu melden ist, unterrichten sie die gemäß den Artikeln 55 und 56 jener Verordnung zuständigen Aufsichtsbehörden ***unverzüglich und in jedem Fall innerhalb von 24 Stunden***.

Änderungsantrag 119

Vorschlag für eine Richtlinie
Artikel 32 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Ist die gemäß der Verordnung (EU) 2016/679 zuständige Aufsichtsbehörde in einem anderen Mitgliedstaat angesiedelt als die zuständige Behörde, so ***kann*** die zuständige Behörde die im selben Mitgliedstaat angesiedelte Aufsichtsbehörde davon in Kenntnis ***setzen***.	(3) Ist die gemäß der Verordnung (EU) 2016/679 zuständige Aufsichtsbehörde in einem anderen Mitgliedstaat angesiedelt als die zuständige Behörde, so ***setzt*** die zuständige Behörde die im selben Mitgliedstaat angesiedelte Aufsichtsbehörde davon in Kenntnis.

Änderungsantrag 120

Vorschlag für eine Richtlinie
Artikel 34 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	Artikel 34 a
	Haftung bei Nichteinhaltung

	Unbeschadet verfügbarer verwaltungsrechtlicher oder außergerichtlicher Rechtsbehelfe haben Empfänger von durch wesentliche oder wichtige Einrichtungen bereitgestellten Diensten, denen aufgrund von Verstößen des Anbieters gegen diese Richtlinie Schäden entstanden sind, das Recht auf einen wirksamen gerichtlichen Rechtsbehelf.

Änderungsantrag 121

Vorschlag für eine Richtlinie
Artikel 35 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
Die Kommission überprüft ***regelmäßig*** die Anwendung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat Bericht. In dem Bericht wird insbesondere die Relevanz der in den Anhängen I und II genannten Sektoren, Teilsektoren und Einrichtungen unterschiedlicher Größe und Art für das Funktionieren der Wirtschaft und Gesellschaft in Bezug auf die Cybersicherheit ***bewertet***. Zu diesem Zweck berücksichtigt die Kommission im Hinblick auf die weitere Förderung der strategischen und operativen Zusammenarbeit die Berichte der Kooperationsgruppe und des CSIRT-Netzwerks über die auf strategischer und operativer Ebene gemachten Erfahrungen. Der erste Bericht dieser Art ist bis zum … ***54*** Monate nach Inkrafttreten dieser Richtlinie vorzulegen.	Die Kommission überprüft ***alle drei Jahre*** die Anwendung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat Bericht. In dem Bericht wird insbesondere ***bewertet, inwieweit die Richtlinie dazu beigetragen hat, ein hohes gemeinsames Maß an Sicherheit und Integrität von Netz- und Informationssystemen sicherzustellen und gleichzeitig das Privatleben und personenbezogene Daten bestmöglich zu schützen, sowie*** die Relevanz der in den Anhängen I und II genannten Sektoren, Teilsektoren und Einrichtungen unterschiedlicher Größe und Art für das Funktionieren der Wirtschaft und Gesellschaft in Bezug auf die Cybersicherheit. Zu diesem Zweck berücksichtigt die Kommission im Hinblick auf die weitere Förderung der strategischen und operativen Zusammenarbeit die Berichte der Kooperationsgruppe und des CSIRT-Netzwerks über die auf strategischer und operativer Ebene gemachten Erfahrungen. Der erste Bericht dieser Art ist bis zum … ***[36*** Monate nach Inkrafttreten dieser Richtlinie***]*** vorzulegen.

Änderungsantrag 122

Vorschlag für eine Richtlinie
Anhang I – Nummer 5 (Gesundheitswesen) – Spiegelstrich 6 (neu)

Vorschlag der Kommission

Sektor	Teilsektor	Art der Einrichtung
5. Gesundheitswesen		– Gesundheitsdienstleister im Sinne des Artikels 3 Buchstabe g der Richtlinie 2011/24/EU[90]
		– EU-Referenzlaboratorien im Sinne des Artikels 15 der Verordnung XXXX/XXXX zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren[91]
		– Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel im Sinne des Artikels 1 Nummer 2 der Richtlinie 2001/83/EG ausüben[92]
		– Einrichtungen, die pharmazeutische Erzeugnisse im Sinne des Abschnitts C Abteilung 21 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) herstellen
		– Einrichtungen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch im Sinne des Artikels 20 der Verordnung XXXX[93] („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden

[91] [Verordnung des Europäischen Parlaments und des Rates zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren und zur Aufhebung des Beschlusses Nr. 1082/2013/EU, Angabe zu aktualisieren nachdem der Vorschlag COM(2020) 727 final angenommen wurde].

[92] Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates vom 6. November 2001 zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel (ABl. L 311 vom 28.11.2001, S. 67).

[93] [Verordnung des Europäischen Parlaments und des Rates zu einer verstärkten Rolle der Europäischen Arzneimittel-Agentur bei der Krisenvorsorge und dem Krisenmanagement in Bezug auf Arzneimittel und Medizinprodukte; Angabe zu aktualisieren nachdem der Vorschlag COM(2020) 725 final angenommen wurde].

Geänderter Text

Sektor	Teilsektor	Art der Einrichtung
		– Gesundheitsdienstleister im Sinne des

5. Gesundheitswesen	Artikels 3 Buchstabe g der Richtlinie 2011/24/EU[90] – EU-Referenzlaboratorien im Sinne des Artikels 15 der Verordnung XXXX/XXXX zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren[91] – Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel im Sinne des Artikels 1 Nummer 2 der Richtlinie 2001/83/EG ausüben[92] – Einrichtungen, die pharmazeutische Erzeugnisse im Sinne des Abschnitts C Abteilung 21 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) herstellen – Einrichtungen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch im Sinne des Artikels 20 der Verordnung XXXX[93] („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden ***– Einrichtungen, die eine Großhandelsgenehmigung im Sinne des Artikels 79 der Richtlinie 2001/83/EG aufweisen***

[91] [Verordnung des Europäischen Parlaments und des Rates zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren und zur Aufhebung des Beschlusses Nr. 1082/2013/EU, Angabe zu aktualisieren nachdem der Vorschlag COM(2020) 727 final angenommen wurde].

[92] Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates vom 6. November 2001 zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel (ABl. L 311 vom 28.11.2001, S. 67).

[93] [Verordnung des Europäischen Parlaments und des Rates zu einer verstärkten Rolle der Europäischen Arzneimittel-Agentur bei der Krisenvorsorge und dem Krisenmanagement in Bezug auf Arzneimittel und Medizinprodukte; Angabe zu aktualisieren nachdem der Vorschlag COM(2020) 725 final angenommen wurde].

VERFAHREN DES MITBERATENDEN AUSSCHUSSES

Titel	Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und Aufhebung der Richtlinie (EU) 2016/1148
Bezugsdokumente – Verfahrensnummer	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Federführender Ausschuss Datum der Bekanntgabe im Plenum	ITRE 21.1.2021
Stellungnahme von Datum der Bekanntgabe im Plenum	LIBE 21.1.2021
Assoziierte Ausschüsse - Datum der Bekanntgabe im Plenum	20.5.2021
Verfasser(in) der Stellungnahme Datum der Benennung	Lukas Mandl 12.4.2021
Prüfung im Ausschuss	16.6.2021 3.9.2021 11.10.2021
Datum der Annahme	12.10.2021
Ergebnis der Schlussabstimmung	+: 44 –: 14 0: 4
Zum Zeitpunkt der Schlussabstimmung anwesende Mitglieder	Magdalena Adamowicz, Katarina Barley, Pernando Barrena Arza, Pietro Bartolo, Nicolas Bay, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Patrick Breyer, Saskia Bricmont, Jorge Buxadé Villalba, Damien Carême, Caterina Chinnici, Clare Daly, Marcel de Graaff, Anna Júlia Donáth, Lena Düpont, Cornelia Ernst, Laura Ferrara, Nicolaus Fest, Maria Grapini, Sophia in ‘t Veld, Patryk Jaki, Marina Kaljurand, Assita Kanko, Fabienne Keller, Peter Kofod, Moritz Körner, Jeroen Lenaers, Juan Fernando López Aguilar, Lukas Mandl, Roberta Metsola, Nadine Morano, Javier Moreno Sánchez, Maite Pagazaurtundúa, Nicola Procaccini, Emil Radev, Paulo Rangel, Terry Reintke, Diana Riba i Giner, Ralf Seekatz, Michal Šimečka, Birgit Sippel, Sara Skyttedal, Martin Sonneborn, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Milan Uhrík, Tom Vandendriessche, Bettina Vollath, Elissavet Vozemberg-Vrionidi, Jadwiga Wiśniewska, Javier Zarzalejos
Zum Zeitpunkt der Schlussabstimmung anwesende Stellvertreter	Olivier Chastel, Tanja Fajon, Jan-Christoph Oetjen, Philippe Olivier, Anne-Sophie Pelletier, Thijs Reuten, Rob Rooken, Maria Walsh

NAMENTLICHE SCHLUSSABSTIMMUNG IM MITBERATENDEN AUSSCHUSS

44	+
ID	Nicolas Bay, Nicolaus Fest, Peter Kofod, Philippe Olivier, Annalisa Tardino, Tom Vandendriessche
NI	Laura Ferrara
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Lena Düpont, Jeroen Lenaers, Lukas Mandl, Roberta Metsola, Nadine Morano, Emil Radev, Paulo Rangel, Ralf Seekatz, Sara Skyttedal, Elissavet Vozemberg-Vrionidi, Maria Walsh, Javier Zarzalejos
Renew	Olivier Chastel, Anna Júlia Donáth, Sophia in 't Veld, Fabienne Keller, Moritz Körner, Jan-Christoph Oetjen, Maite Pagazaurtundúa, Michal Šimečka, Ramona Strugariu
S&D	Katarina Barley, Pietro Bartolo, Caterina Chinnici, Tanja Fajon, Maria Grapini, Marina Kaljurand, Juan Fernando López Aguilar, Javier Moreno Sánchez, Thijs Reuten, Birgit Sippel, Bettina Vollath
Verts/ALE	Damien Carême

14	-
ECR	Jorge Buxadé Villalba, Patryk Jaki, Assita Kanko, Nicola Procaccini, Rob Rooken, Jadwiga Wiśniewska
ID	Marcel de Graaff
NI	Martin Sonneborn, Milan Uhrík
Verts/ALE	Patrick Breyer, Saskia Bricmont, Terry Reintke, Diana Riba i Giner, Tineke Strik

4	0
The Left	Pernando Barrena Arza, Clare Daly, Cornelia Ernst, Anne-Sophie Pelletier

Erläuterungen:
+ : dafür
- : dagegen
0 : Enthaltung

15.7.2021

STELLUNGNAHME DES AUSSCHUSSES FÜR AUSWÄRTIGE ANGELEGENHEITEN

für den Ausschuss für Industrie, Forschung und Energie

zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148
(2020/0359(COD))

Verfasserin der Stellungnahme: Markéta Gregorová

ÄNDERUNGSANTRÄGE

Der Ausschuss für auswärtige Angelegenheiten ersucht den federführenden Ausschuss für Industrie, Forschung und Energie, folgende Änderungsanträge zu berücksichtigen:

Änderungsantrag 1

Vorschlag für eine Richtlinie
Erwägung 2

Vorschlag der Kommission	*Geänderter Text*
(2) Seit Inkrafttreten der Richtlinie (EU) 2016/1148 sind erhebliche Fortschritte bei der Stärkung der Cyberresilienz der Union erzielt worden. Die Überprüfung jener Richtlinie hat gezeigt, dass sie als Katalysator für das institutionelle und regulatorische Cybersicherheitskonzept in der Union gedient und ein erhebliches Umdenken bewirkt hat. Durch die Festlegung nationaler Cybersicherheitsstrategien, die Schaffung nationaler Kapazitäten und die Umsetzung von Regulierungsmaßnahmen	(2) Seit Inkrafttreten der Richtlinie (EU) 2016/1148 sind erhebliche Fortschritte bei der Stärkung der Cyberresilienz der Union erzielt worden. Die Überprüfung jener Richtlinie hat gezeigt, dass sie als Katalysator für das institutionelle und regulatorische Cybersicherheitskonzept in der Union gedient und ein erhebliches Umdenken bewirkt hat. Durch die Festlegung nationaler Cybersicherheitsstrategien, die Schaffung nationaler Kapazitäten und die Umsetzung von Regulierungsmaßnahmen

für Infrastrukturen und Akteure, die von den einzelnen Mitgliedstaaten als wesentlich eingestuft wurden, wurde mit jener Richtlinie die Vervollständigung der nationalen Rechtsrahmen sichergestellt. Darüber hinaus hat sie durch die Einrichtung der Kooperationsgruppe[12] und eines Netzwerks nationaler Reaktionsteams für IT-Sicherheitsvorfälle (CSIRT-Netzwerk)[13] zur Zusammenarbeit auf Unionsebene beigetragen. Ungeachtet dieser Erfolge hat die Überprüfung der Richtlinie (EU) 2016/1148 inhärente Mängel ergeben, die ein wirksames Vorgehen gegen aktuelle und neue Herausforderungen im Bereich Cybersicherheit verhindern.

für Infrastrukturen und Akteure, die von den einzelnen Mitgliedstaaten als wesentlich eingestuft wurden, wurde mit jener Richtlinie die Vervollständigung der nationalen Rechtsrahmen sichergestellt. Darüber hinaus hat sie durch die Einrichtung der Kooperationsgruppe[12] und eines Netzwerks nationaler Reaktionsteams für IT-Sicherheitsvorfälle (CSIRT-Netzwerk)[13] zur Zusammenarbeit auf Unionsebene beigetragen. ***Die Richtlinie (EU) 2016/1148 war der erste unionsweite Rechtsakt zur Cybersicherheit, der rechtliche Maßnahmen vorsah, um das allgemeine Niveau der Cyberresilienz, auch im Bereich der Sicherheit und Verteidigung in der Union, zu steigern, indem für Zusammenarbeit unter den Mitgliedstaaten und eine Kultur der sektorübergreifenden Sicherheit gesorgt wurde.*** Ungeachtet dieser Erfolge hat die Überprüfung der Richtlinie (EU) 2016/1148 inhärente Mängel ergeben, die ein wirksames Vorgehen gegen aktuelle und neue Herausforderungen im Bereich Cybersicherheit***, die sehr häufig ihren Ursprung außerhalb der Union haben und eine ernsthafte Bedrohung für die innere und äußere Sicherheit auf Unionsebene darstellen,*** verhindern.

[12] Artikel 11 der Richtlinie (EU) 2016/1148.

[13] Artikel 12 der Richtlinie (EU) 2016/1148.

[12] Artikel 11 der Richtlinie (EU) 2016/1148.

[13] Artikel 12 der Richtlinie (EU) 2016/1148.

Änderungsantrag 2

Vorschlag für eine Richtlinie
Erwägung 3 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(3a) Hybride Kampagnen sind nach Auffassung der Union „multidimensional, kombinieren Zwangsausübung mit

subversiven Maßnahmen und nutzen zur Destabilisierung des Gegners sowohl konventionelle als auch nicht konventionelle Mittel und Taktiken auf diplomatischer, militärischer, wirtschaftlicher und technologischer Ebene. Sie sind so konzipiert, dass sie schwer aufzudecken oder jemandem zuzuordnen sind und können sowohl von staatlichen als auch nichtstaatlichen Akteuren ausgehen“[1a]. Das Internet und Online-Netze bieten staatlichen und nichtstaatlichen Akteuren neue Möglichkeiten für ein aggressives Vorgehen. Sie können genutzt werden, um kritische Infrastrukturen und demokratische Prozesse zu hacken, überzeugende Desinformations- und Propagandakampagnen einzuleiten, Informationen zu stehlen und sensible Daten an die Öffentlichkeit zu bringen. In den schlimmsten Fällen ermöglichen Cyberangriffe es einem Gegner, die Kontrolle über Anlagen wie militärische Systeme und Führungsstrukturen zu erlangen[1b]. Gleichzeitig ist die eingehende Zusammenarbeit mit dem Privatsektor und zivilen Akteuren, einschließlich der Industrie und Stellen, die an der Verwaltung kritischer Infrastrukturen beteiligt sind, maßgeblich und sollte aufgrund der inhärenten Merkmale des Cyberbereichs, in dem technologische Innovationen hauptsächlich von privaten Unternehmen vorangetrieben werden, die oft nicht im militärischen Bereich tätig sind, verstärkt werden. Zur Vorbereitung für und zum Schutz gegen derartige Cybersicherheitsvorfälle und -krisen großen Ausmaßes auf Unionsebene müssen angemessene Vorkehrungen im Rahmen gemeinsamer Schulungsmaßnahmen getroffen werden, da in einem solchen Fall Artikel 222 AEUV („Solidaritätsklausel“) geltend gemacht werden kann.

[1a] Kommission/Hohe Vertreterin der Union für Außen- und Sicherheitspolitik, Gemeinsame Mitteilung mit dem Titel „Stärkung der Resilienz und Ausbau der Kapazitäten zur Abwehr hybrider Bedrohungen", JOIN(2018)0016, Brüssel, 13. Juni 2018, S. 1.

[1b]

https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_151.pdf

Änderungsantrag 3

Vorschlag für eine Richtlinie
Erwägung 3 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	(3b) Bei Cybersicherheitsvorfällen und -krisen großen Ausmaßes auf Unionsebene ist aufgrund der starken gegenseitigen Abhängigkeit von Sektoren und Staaten ein koordiniertes Vorgehen erforderlich, um eine rasche und wirksame Reaktion sowie eine bessere Prävention und Vorbereitung auf ähnliche Situationen in der Zukunft sicherzustellen. Die Verfügbarkeit von cyber-resilienten Netzen und Informationssystemen und die Verfügbarkeit, Vertraulichkeit und Integrität von Daten sind für die Sicherheit innerhalb der Union und jenseits ihrer Grenzen von entscheidender Bedeutung. Das Bestreben der Union, eine stärkere geopolitische Rolle einzunehmen, hängt auch von einer glaubwürdigen Cyberabwehr und -abschreckung ab, wozu auch die Fähigkeit gehört, böswillige Handlungen rechtzeitig wirksam zu erkennen und angemessen darauf zu reagieren. Angesichts der verschwimmenden Grenzen zwischen zivilen und militärischen Angelegenheiten und des doppelten Verwendungszwecks von Cyberinstrumenten und -technologien bedarf es eines umfassenden und

ganzheitlichen Konzepts für den Digitalbereich. Dies gilt auch für Missionen und Operationen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP), die von der Union durchgeführt werden, um in ihrer Nachbarschaft und darüber hinaus für Frieden und Stabilität zu sorgen. In diesem Zusammenhang sollte der Strategische Kompass der Union dazu dienen, die Umsetzung der ehrgeizigen Ziele der Union in den Bereichen Sicherheit und Verteidigung zu verbessern und zu lenken und diese Ziele auf den Bedarf an Fähigkeiten im Bereich der Cyberverteidigung zu übertragen, wodurch die Union und die Mitgliedstaaten besser in der Lage sein werden, böswillige Cyberaktivitäten zu verhindern, davon abzuschrecken, darauf zu reagieren und sich davon zu erholen, indem sie ihre Haltung, ihr Situationsbewusstsein, ihre Instrumente, ihre Verfahren und ihre Partnerschaften stärken. Die Zusammenarbeit der Union mit internationalen Organisationen wie der NATO trägt zu Gesprächen über Möglichkeiten der Prävention, Abschreckung und Reaktion auf hybride Angriffe und Cyberangriffe und zur Prüfung von Wegen zur Einrichtung einer gemeinsamen Cyberbedrohungsanalyse bei.

Änderungsantrag 4

Vorschlag für eine Richtlinie
Erwägung 6

Vorschlag der Kommission	*Geänderter Text*
(6) Im Einklang mit dem Unionsrecht bleibt die Möglichkeit der Mitgliedstaaten, die für die Wahrung ihrer wesentlichen Sicherheitsinteressen und den Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit erforderlichen Maßnahmen zu ergreifen und die Ermittlung, Feststellung	(6) Im Einklang mit dem Unionsrecht ***und den Grundrechten*** bleibt die Möglichkeit der Mitgliedstaaten, die für die Wahrung ihrer wesentlichen Sicherheitsinteressen und den Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit erforderlichen Maßnahmen zu

und Verfolgung von Straftaten zuzulassen, von der vorliegenden Richtlinie unberührt. Nach Artikel 346 AEUV ist kein Mitgliedstaat verpflichtet, Auskünfte zu erteilen, deren Preisgabe seinen wesentlichen Sicherheitsinteressen widerspräche. In diesem Zusammenhang sind nationale und Unionsvorschriften zum Schutz von Verschlusssachen, Geheimhaltungsvereinbarungen und informelle Geheimhaltungsvereinbarungen wie das sogenannte Traffic Light Protocol[14] von Bedeutung.

[14] Mithilfe des Traffic Light Protocol (TLP) kann jemand, der Informationen weitergibt, die Empfänger über etwaige Einschränkungen bei der weiteren Verbreitung dieser Informationen informieren. Es wird in fast allen CSIRT-Gemeinschaften und einigen Informationsaustausch- und -analysezentren (Information Sharing and Analysis Centres – ISACs) genutzt.

ergreifen und die Ermittlung, Feststellung und Verfolgung von Straftaten zuzulassen, von der vorliegenden Richtlinie unberührt. ***Unabhängig vom technologischen Umfeld ist es unerlässlich, ordnungsgemäße Verfahren und sonstige Garantien, insbesondere die Grundrechte, etwa das Recht auf Achtung des Privatlebens und der privaten Kommunikation und das Recht auf den Schutz personenbezogener Daten, uneingeschränkt zu achten. Ebenso sind zur Sicherstellung einer umfassenden Widerstandsfähigkeit nicht nur die Stärkung der technologischen Infrastrukturen und der Besitz von Reaktionskapazitäten, sondern auch eine Sensibilisierung der Öffentlichkeit für Cyberrisiken und -sicherheit erforderlich.*** Nach Artikel 346 AEUV ist kein Mitgliedstaat verpflichtet, Auskünfte zu erteilen, deren Preisgabe seinen wesentlichen Sicherheitsinteressen widerspräche. In diesem Zusammenhang sind nationale und Unionsvorschriften zum Schutz von Verschlusssachen, Geheimhaltungsvereinbarungen und informelle Geheimhaltungsvereinbarungen wie das sogenannte Traffic Light Protocol[14] von Bedeutung.

[14] Mithilfe des Traffic Light Protocol (TLP) kann jemand, der Informationen weitergibt, die Empfänger über etwaige Einschränkungen bei der weiteren Verbreitung dieser Informationen informieren. Es wird in fast allen CSIRT-Gemeinschaften und einigen Informationsaustausch- und -analysezentren (Information Sharing and Analysis Centres – ISACs) genutzt.

Änderungsantrag 5

Vorschlag für eine Richtlinie
Erwägung 14 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(14a) Mit Blick auf die Entwicklung eines sicheren Konnektivitätssystems und den Aufbau auf der europäischen Quantenkommunikationsinfrastruktur (EuroQCI) und der staatlichen Satellitenkommunikation in der Europäischen Union (GOVSATCOM), insbesondere die Umsetzung des globalen Satellitennavigationssystems (GNSS) GALILEO für Nutzer im Verteidigungsbereich, in dem bei möglichen künftigen Entwicklungen unter anderem die Auswirkungen der Kombination der Geschwindigkeit und Ausgereiftheit der Quanteninformatik mit hochgradig autonomen militärischen Systemen zu berücksichtigen sind, sollten die Mitgliedstaaten den Schutz der gesamten elektronischen Kommunikationsinfrastruktur, etwa von Weltraum-, Land- und Unterseenetzen sicherstellen. Gleichzeitig sollte eine gemeinsame Vision in Bezug auf die Strategie zur Cloud-Einführung für sensible Sektoren festgelegt werden, wobei das Ziel darin besteht, einen Ansatz der Union zu erarbeiten, der auf gemeinsamen Standards unter gleichgesinnten Partnerländern beruht.

Änderungsantrag 6

Vorschlag für eine Richtlinie
Erwägung 20

Vorschlag der Kommission	*Geänderter Text*
(20) Diese wachsenden gegenseitigen Abhängigkeiten sind das Ergebnis eines sich über immer mehr Grenzen hinweg erstreckenden und zunehmend interdependenten Dienstleistungsnetzes, das zentrale Infrastrukturen in der gesamten Union nutzt, und zwar in den Sektoren Energie, Verkehr, digitale Infrastruktur, Trinkwasser und Abwasser,	(20) Diese wachsenden gegenseitigen Abhängigkeiten sind das Ergebnis eines sich über immer mehr Grenzen hinweg erstreckenden und zunehmend interdependenten Dienstleistungsnetzes, das zentrale Infrastrukturen in der gesamten Union nutzt, und zwar in den Sektoren Energie, Verkehr, digitale Infrastruktur, Trinkwasser und Abwasser,

Gesundheit, bestimmten Bereichen der öffentlichen Verwaltung sowie im Weltraumsektor, soweit es um die Erbringung bestimmter Dienste geht, die von Bodeninfrastrukturen abhängig sind, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden; damit sind Infrastrukturen ausgenommen, die sich im Eigentum der Union befinden oder von der Union oder in ihrem Namen im Rahmen ihrer Weltraumprogramme verwaltet oder betrieben werden. Wegen dieser gegenseitigen Abhängigkeiten kann jede Störung, auch wenn sie anfänglich auf eine Einrichtung oder einen Sektor beschränkt ist, zu breiteren Kaskadeneffekten führen, die weitreichende und lang anhaltende negative Auswirkungen auf die Erbringung von Dienstleistungen im gesamten Binnenmarkt haben können. Die COVID-19-Pandemie hat gezeigt, wie anfällig unsere zunehmend interdependenten Gesellschaften für Risiken mit geringer Eintrittswahrscheinlichkeit sind.

Gesundheit, bestimmten Bereichen der öffentlichen Verwaltung sowie im Weltraumsektor, soweit es um die Erbringung bestimmter Dienste geht, die von Bodeninfrastrukturen abhängig sind, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden; damit sind Infrastrukturen ausgenommen, die sich im Eigentum der Union befinden oder von der Union oder in ihrem Namen im Rahmen ihrer Weltraumprogramme verwaltet oder betrieben werden. ***Infrastruktur, die sich im Eigentum der Union befindet oder von der Union oder in ihrem Namen im Rahmen ihrer Weltraumprogramme verwaltet oder betrieben wird, ist für die Sicherheit der Union und ihrer Mitgliedstaaten sowie das ordnungsgemäße Funktionieren der GSVP-Missionen besonders wichtig. Infrastruktur dieser Art muss im Einklang mit der Verordnung (EU) 2021/696 des Europäischen Parlaments und des Rates[18a] angemessen geschützt werden.*** Wegen dieser gegenseitigen Abhängigkeiten kann jede Störung, auch wenn sie anfänglich auf eine Einrichtung oder einen Sektor beschränkt ist, zu breiteren Kaskadeneffekten führen, die weitreichende und lang anhaltende negative Auswirkungen auf die Erbringung von Dienstleistungen im gesamten Binnenmarkt haben können ***und die Sicherheit der Unionsbürger gefährden***. Die COVID-19-Pandemie hat gezeigt, wie anfällig unsere zunehmend interdependenten Gesellschaften für Risiken mit geringer Eintrittswahrscheinlichkeit sind.

18a Verordnung (EU) 2021/696 des Europäischen Parlaments und des Rates vom 28. April 2021 zur Einrichtung des Weltraumprogramms der Union und der Agentur der Europäischen Union für das Weltraumprogramm und zur Aufhebung der Verordnungen (EU) Nr. 912/2010,

(EU) Nr. 1285/2013 und (EU) Nr. 377/2014 sowie des Beschlusses Nr. 541/2014/EU (ABl. L 170 vom 12.5.2021, S. 69).

Änderungsantrag 7

Vorschlag für eine Richtlinie
Erwägung 26

Vorschlag der Kommission	*Geänderter Text*
(26) Wegen der Bedeutung der internationalen Zusammenarbeit im Bereich Cybersicherheit sollten die CSIRTs sich zusätzlich zum durch die vorliegende Richtlinie geschaffenen CSIRT-Netzwerk an internationalen Kooperationsnetzen beteiligen können.	(26) Wegen der Bedeutung der internationalen Zusammenarbeit im Bereich Cybersicherheit sollten die CSIRTs sich zusätzlich zum durch die vorliegende Richtlinie geschaffenen CSIRT-Netzwerk an internationalen Kooperationsnetzen beteiligen können***, um zur Erarbeitung von Normen der Union beizutragen, die die Cybersicherheitslandschaft auf internationaler Ebene prägen können. Die Mitgliedstaaten sollten auch die Möglichkeiten einer verstärkten Zusammenarbeit mit gleichgesinnten Partnerländern und internationalen Organisationen wie dem Europarat, der Nordatlantikvertrags-Organisation, der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung, der Organisation für Sicherheit und Zusammenarbeit in Europa und den Vereinten Nationen prüfen, um multilaterale Vereinbarungen über Normen für den Cyberbereich, verantwortungsbewusstes staatliches und nichtstaatliches Verhalten im Cyberraum und eine wirksame globale E-Governance sicherzustellen und einen offenen, freien, stabilen und sicheren Cyberraum auf der Grundlage des Völkerrechts zu schaffen.***

Änderungsantrag 8

Vorschlag für eine Richtlinie
Erwägung 27

Vorschlag der Kommission	*Geänderter Text*
(27) Im Einklang mit dem Anhang der Empfehlung (EU) 2017/1548 der Kommission für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen („Konzeptentwurf“)[20] sollte der Begriff „Sicherheitsvorfall großen Ausmaßes“ einen Sicherheitsvorfall bezeichnen, der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat oder der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt. Je nach Ursache und Auswirkung können sich Sicherheitsvorfälle großen Ausmaßes verschärfen und zu echten Krisen entwickeln, die das reibungslose Funktionieren des Binnenmarkts verhindern. Angesichts der großen Tragweite und des, in den meisten Fällen, grenzübergreifenden Charakters solcher Sicherheitsvorfälle sollten die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union auf technischer, operativer und politischer Ebene zusammenarbeiten, um die Reaktion unionsweit angemessen zu koordinieren.	(27) Im Einklang mit dem Anhang der Empfehlung (EU) 2017/1548 der Kommission für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen („Konzeptentwurf“)[20] sollte der Begriff „Sicherheitsvorfall großen Ausmaßes“ einen Sicherheitsvorfall bezeichnen, der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat oder der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt. Je nach Ursache und Auswirkung können sich Sicherheitsvorfälle großen Ausmaßes verschärfen und zu echten Krisen entwickeln, die das reibungslose Funktionieren des Binnenmarkts verhindern ***oder die Sicherheit der Bürger sowie die wirtschaftlichen und finanziellen Interessen der Union gefährden***. Angesichts der großen Tragweite und des, in den meisten Fällen, grenzübergreifenden Charakters solcher Sicherheitsvorfälle sollten die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union auf technischer, operativer und politischer Ebene zusammenarbeiten, um die Reaktion unionsweit angemessen zu koordinieren. ***Die Union und die Mitgliedstaaten sollten auch weiter Übungen und szenariobasierte politische Debatten über Rahmen für das Krisenmanagement fördern, um interne und externe Politikkohärenz sicherzustellen und ein gemeinsames Verständnis der Verfahren für die Anwendung der Solidaritätsklausel zu schaffen.***
[20] Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (ABl. L 239 vom 19.9.2017, S. 36).	[20] Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (ABl. L 239 vom 19.9.2017, S. 36).

Änderungsantrag 9

Vorschlag für eine Richtlinie
Erwägung 36

Vorschlag der Kommission	*Geänderter Text*
(36) Die Union sollte gegebenenfalls internationale Übereinkünfte mit Drittländern oder internationalen Organisationen im Einklang mit Artikel 218 AEUV schließen, in denen deren Beteiligung an bestimmten Tätigkeiten der Kooperationsgruppe und dem CSIRT-Netzwerk ermöglicht und geregelt wird. Solche Übereinkünfte ***sollten*** einen angemessenen Datenschutz gewährleisten.	(36) Die Union sollte gegebenenfalls internationale Übereinkünfte mit Drittländern oder internationalen Organisationen im Einklang mit Artikel 218 AEUV schließen, in denen deren Beteiligung an bestimmten Tätigkeiten der Kooperationsgruppe und dem CSIRT-Netzwerk ermöglicht und geregelt wird. Solche Übereinkünfte ***sollen*** einen angemessenen Datenschutz gewährleisten***, den Markzugang fördern sowie Sicherheitsrisiken entgegenwirken und zugleich die globale Resilienz steigern und das Bewusstsein für Cyberbedrohungen und böswillige Cyberaktivitäten schärfen. Die Union sollte auch weiterhin den Kapazitätsaufbau in Drittländern unterstützen. Die Mitgliedstaaten sollten gegebenenfalls die Beteiligung gleichgesinnter Partnerländer, die die Werte der Union teilen, an einschlägigen SSZ-Projekten fördern. Daher sollte die Kommission prüfen, ob erneut Verfahren eingeleitet werden können, um formale und strukturierte Rahmen für die künftige Zusammenarbeit in diesem Bereich zu schaffen.***

Änderungsantrag 10

Vorschlag für eine Richtlinie
Erwägung 37

Vorschlag der Kommission	*Geänderter Text*
(37) Die Mitgliedstaaten sollten über die bestehenden Kooperationsnetzwerke – insbesondere das Netzwerk der	(37) Die Mitgliedstaaten sollten über die bestehenden Kooperationsnetzwerke – insbesondere das Netzwerk der

Verbindungsorganisationen für Cyberkrisen (Cyber Crisis Liaison Organisation Network, EU-CyCLONe), das CSIRT-Netzwerk und die Kooperationsgruppe – zur Schaffung des EU-Rahmens für die Reaktion auf Cybersicherheitskrisen gemäß der Empfehlung (EU) 2017/1584 beitragen. EU-CyCLONe und das CSIRT-Netzwerk sollten auf der Grundlage von verfahrenstechnischen Vereinbarungen zusammenarbeiten, in denen die Modalitäten dieser Zusammenarbeit festgelegt werden. In der Geschäftsordnung von EU-CyCLONe sollten die Modalitäten für das Funktionieren des Netzwerks genauer festgelegt werden, einschließlich, aber nicht beschränkt auf Funktion und Aufgaben, Formen der Zusammenarbeit, Interaktionen mit anderen relevanten Akteuren und Vorlagen für den Informationsaustausch sowie Kommunikationsmittel. Für das Krisenmanagement auf Unionsebene sollten sich die relevanten Parteien auf die Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) stützen. Die Kommission sollte zu diesem Zweck auf den sektorübergreifenden Krisenkoordinierungsprozess auf hoher Ebene, ARGUS, zurückgreifen. Berührt die Krise eine wichtige externe Dimension oder eine Dimension der ***Gemeinsamen Sicherheits- und Verteidigungspolitik (***GSVP***)***, so ***sollte*** der Krisenreaktionsmechanismus des Europäischen Auswärtigen Dienstes (EAD) ausgelöst werden.

Verbindungsorganisationen für Cyberkrisen (Cyber Crisis Liaison Organisation Network, EU-CyCLONe), das CSIRT-Netzwerk und die Kooperationsgruppe***, das Europäische Zentrum zur Bekämpfung der Cyberkriminalität und das Zentrum der Union für Informationsgewinnung und Lageerfassung (EU INTCEN)*** – zur Schaffung des EU-Rahmens für die Reaktion auf Cybersicherheitskrisen gemäß der Empfehlung (EU) 2017/1584 beitragen***, um die strategische nachrichtendienstliche Zusammenarbeit in Bezug auf Cyberbedrohungen und -aktivitäten voranzubringen und so die Lageerfassung der Union und die Beschlussfassung im Hinblick auf eine gemeinsame diplomatische Reaktion weiter zu unterstützen***. EU-CyCLONe und das CSIRT-Netzwerk sollten auf der Grundlage von verfahrenstechnischen Vereinbarungen zusammenarbeiten, in denen die Modalitäten dieser Zusammenarbeit festgelegt werden. In der Geschäftsordnung von EU-CyCLONe sollten die Modalitäten für das Funktionieren des Netzwerks genauer festgelegt werden, einschließlich, aber nicht beschränkt auf Funktion und Aufgaben, Formen der Zusammenarbeit, Interaktionen mit anderen relevanten Akteuren und Vorlagen für den Informationsaustausch sowie Kommunikationsmittel. Für das Krisenmanagement auf Unionsebene sollten sich die relevanten Parteien auf die Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) stützen***, mit der auch auf politischer Ebene die Koordinierung der Reaktion auf die Geltendmachung der Solidaritätsklausel unterstützt wird***. Die Kommission sollte zu diesem Zweck auf den sektorübergreifenden Krisenkoordinierungsprozess auf hoher Ebene, ARGUS, zurückgreifen. Berührt die Krise eine wichtige externe Dimension oder eine Dimension der GSVP, so ***sollten***

der Krisenreaktionsmechanismus des Europäischen Auswärtigen Dienstes (EAD) ***sowie Maßnahmen zum Schutz der Missionen und Operationen im Rahmen der GSVP und der Delegationen der Union*** ausgelöst werden. ***Des Weiteren sollte die Union ihr Instrumentarium im Bereich der Cyberdiplomatie in vollem Umfang nutzen.***

Änderungsantrag 11

Vorschlag für eine Richtlinie
Erwägung 40 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(40a) Im Rahmen ihrer nationalen Cybersicherheitsstrategie sollten die Mitgliedstaaten ein Programm der aktiven Cyberabwehr in Betracht ziehen, das regelmäßige gemeinsame Schulungsmaßnahmen unter Mitgliedstaaten und internationalen Organisationen umfasst. Ein derartiges Programm sollte die Möglichkeit bieten, Bedrohungen synchronisiert und in Echtzeit zu entdecken, zu erkennen, zu analysieren und zu mindern. Aktive Cyberabwehr wird bei Netzgeschwindigkeit mithilfe von Sensoren, Software und Informationen betrieben, um böswillige Aktivitäten zu erkennen und aufzuhalten, idealerweise bevor sie Netze und Systeme beeinträchtigen können. Darüber hinaus sollten die Mitgliedstaaten das Verfahren des Informationsaustauschs deutlich verbessern und einen gemeinsamen Kommunikationsstandard festlegen, der für Verschlusssachen und andere Informationen verwendet werden könnte, um für ein rasches Handeln zu sorgen. Zur wirksamen Abschreckung und verhältnismäßigen Reaktion auf Cyberangriffe im Einklang mit dem Völkerrecht sollten die Union und die Mitgliedstaaten auch ihre Kapazitäten für

deren Zuordnung stärken.

Änderungsantrag 12

Vorschlag für eine Richtlinie
Erwägung 40 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	(40b) Die Mitgliedstaaten sollten im Rahmen ihrer nationalen Cybersicherheitsstrategien ein Programm der aktiven Cyberabwehr vorlegen. Aktive Cyberabwehr bezeichnet die proaktive Erkennung, Analyse und Minderung von Verstößen im Bereich der Netzsicherheit in Echtzeit in Verbindung mit der Nutzung von Kapazitäten außerhalb des betroffenen Netzes. Sie beruht auf einer Abwehrstrategie, bei der offensive Maßnahmen gegen die kritische zivile Infrastruktur der Gegner, die einen Verstoß gegen das Völkerrecht (etwa gegen das Zusatzprotokoll zu den Genfer Abkommen von 1977) darstellen würden, ausgeschlossen sind. Die Fähigkeit, Bedrohungsinformationen und -analysen, Warnungen in Bezug auf Cyberaktivitäten und Gegenmaßnahmen rasch und automatisch auszutauschen und zu verstehen, ist von entscheidender Bedeutung, um eine Bündelung der Anstrengungen zur erfolgreichen Erkennung und Prävention von Cyberangriffen zu ermöglichen. Zu den Aktivitäten der aktiven Cyberabwehr könnten Konfigurationen von E-Mail-Servern und Websites, die Aktivierung der Protokollierung und die DNS-Filterung gehören. Die Mitgliedstaaten sollten Maßnahmen ergreifen, um einen möglichst umfassenden Zugang zu den leistungsfähigsten Cybersicherheitsinstrumenten sicherzustellen und Unternehmen, kleine und mittlere Unternehmen und Unternehmen mit geringen finanziellen Möglichkeiten durch Vergünstigungen,

	Zuschüsse, Darlehen oder steuerliche Vorteile, die für den Erwerb erstklassiger Cybersicherheitsprodukte und -dienstleistungen bestimmt sind, zu unterstützen, wobei zu vermeiden ist, dass deren Kosten ein diskriminierendes Element darstellen. Die Mitgliedstaaten sollten ferner bestrebt sein, Partnerschaften mit Hochschuleinrichtungen und anderen Forschungseinrichtungen zu fördern, mit denen Forschungs- und Entwicklungsprogramme im Bereich der Cybersicherheit unterstützt werden, um im Rahmen eines multidisziplinären Ansatzes neue gemeinsame Technologien, Instrumente und Kompetenzen zu entwickeln, die sowohl im zivilen als auch im Verteidigungsbereich anwendbar sind. Diese Partnerschaften sollten aus bestehenden und neuen Finanzierungsinstrumenten unter der Schirmherrschaft der Kommission finanziert werden.

Änderungsantrag 13

Vorschlag für eine Richtlinie
Erwägung 43

Vorschlag der Kommission	*Geänderter Text*
(43) Besonders wichtig ist die Bewältigung von Cybersicherheitsrisiken, die die Lieferkette von Einrichtungen und deren Beziehungen zu den Lieferanten betreffen, da sich die Vorfälle häufen, bei denen Einrichtungen Opfer von Cyberangriffen werden und es böswilligen Akteuren gelingt, die Sicherheit der Netz- und Informationssysteme zu beeinträchtigen, indem Schwachstellen im Zusammenhang mit den Produkten und Dienstleistungen Dritter ausgenutzt werden. Die Einrichtungen sollten daher die Gesamtqualität der Produkte und Cybersicherheitsverfahren ihrer Lieferanten und Diensteanbieter,	(43) Besonders wichtig ist die Bewältigung von Cybersicherheitsrisiken, die die Lieferkette von Einrichtungen und deren Beziehungen zu den Lieferanten betreffen, da sich die Vorfälle häufen, bei denen Einrichtungen Opfer von Cyberangriffen werden und es böswilligen Akteuren gelingt, die Sicherheit der Netz- und Informationssysteme zu beeinträchtigen, indem Schwachstellen im Zusammenhang mit den Produkten und Dienstleistungen Dritter ausgenutzt werden. Die Einrichtungen sollten daher die Gesamtqualität der Produkte und Cybersicherheitsverfahren ihrer Lieferanten und Diensteanbieter,

einschließlich ihrer sicheren Entwicklungsprozesse, bewerten und berücksichtigen.

einschließlich ihrer ***Risikomanagement-Systeme und*** sicheren Entwicklungsprozesse, ***im Einklang mit den Cybersicherheitsstandards der Union*** bewerten und berücksichtigen.

Änderungsantrag 14

Vorschlag für eine Richtlinie
Erwägung 43 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(43a) Zu den potenziellen nichttechnischen Risikofaktoren wie ungebührlicher Einflussnahme eines Drittlandes auf Lieferanten und Diensteanbieter, insbesondere im Fall von alternativen Governance-Modellen, zählen versteckte Schwachstellen oder Hintertüren sowie potenzielle systemische Versorgungsunterbrechungen, insbesondere im Fall von Zwangsbindungen an bestimmte Technologien oder Anbieter. Da durch die Ausnutzung von Schwachstellen im Verteidigungsbereich erhebliche Störungen und Schäden verursacht werden können, sind im Bereich der Cybersicherheit der Verteidigungsindustrie besondere Maßnahmen erforderlich, um die Sicherheit von Lieferketten, insbesondere von weiter unten in der Lieferkette stehenden Einrichtungen, die keinen Zugang zu Verschlusssachen benötigen, aber ernsthafte Risiken für den gesamten Sektor bergen könnten, sicherzustellen. Den Auswirkungen von Verstößen sowie der Bedrohung durch potenzielle Manipulationen von Netzwerkdaten, durch die kritische Verteidigungsanlagen unbrauchbar gemacht oder sogar ihre Betriebssysteme ausgeschaltet werden könnten, sodass sie anfällig sind für eine Übernahme, sollte besondere Aufmerksamkeit gewidmet werden.

Änderungsantrag 15

Vorschlag für eine Richtlinie
Erwägung 46

Vorschlag der Kommission	*Geänderter Text*
(46) Um die Hauptrisiken für die Lieferkette weiter anzugehen und den Einrichtungen in den unter diese Richtlinie fallenden Sektoren dabei zu helfen, Cybersicherheitsrisiken in Bezug auf die Lieferkette und die Lieferanten angemessen zu beherrschen, sollte die Kooperationsgruppe, an der die einschlägigen nationalen Behörden beteiligt sind, in Zusammenarbeit mit der Kommission ***und*** der ENISA koordinierte sektorenbezogene Lieferketten-Risikobewertungen – wie im Fall der 5G-Netze gemäß der einschlägigen Empfehlung (EU) 2019/534***[46]*** – durchführen, um für jeden Sektor die kritischen IKT-Dienste, -Systeme oder -Produkte sowie relevante Bedrohungen und Schwachstellen zu ermitteln.	(46) Um die Hauptrisiken für die Lieferkette weiter anzugehen und den Einrichtungen in den unter diese Richtlinie fallenden Sektoren dabei zu helfen, Cybersicherheitsrisiken in Bezug auf die Lieferkette und die Lieferanten angemessen zu beherrschen, sollte die Kooperationsgruppe, an der die einschlägigen nationalen Behörden beteiligt sind, in Zusammenarbeit mit der Kommission***,*** der ENISA ***und dem Europäischen Auswärtigen Dienst*** koordinierte sektorenbezogene Lieferketten-Risikobewertungen – wie im Fall der 5G-Netze gemäß der einschlägigen Empfehlung (EU) 2019/534***[21]*** – durchführen, um für jeden Sektor die kritischen IKT-Dienste, -Systeme oder -Produkte sowie relevante Bedrohungen und Schwachstellen zu ermitteln.
[21] Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019 Cybersicherheit der 5G-Netze (ABl. L 88 vom 29.3.2019, S. 42).	[21] Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019 Cybersicherheit der 5G-Netze (ABl. L 88 vom 29.3.2019, S. 42).

Änderungsantrag 16

Vorschlag für eine Richtlinie
Erwägung 68

Vorschlag der Kommission	*Geänderter Text*
(68) Die Einrichtungen sollten ermutigt werden, ihre individuellen Kenntnisse und praktischen Erfahrungen auf strategischer, taktischer und operativer Ebene gemeinsam zu nutzen, damit sich ihre	(68) Die Einrichtungen sollten ermutigt werden, ihre individuellen Kenntnisse und praktischen Erfahrungen auf strategischer, taktischer und operativer Ebene gemeinsam zu nutzen, damit sich ihre

Fähigkeit verbessert, Cyberbedrohungen angemessen zu bewerten, zu überwachen, abzuwehren und auf sie zu reagieren. Daher muss dafür gesorgt werden, dass auf Unionsebene Mechanismen für Vereinbarungen über den freiwilligen Informationsaustausch entstehen können. Zu diesem Zweck sollten die Mitgliedstaaten auch einschlägige Einrichtungen, die nicht unter diese Richtlinie fallen, aktiv unterstützen und dazu anhalten, sich an solchen Mechanismen zum Informationsaustausch zu beteiligen. Diese Mechanismen sollten unter uneingeschränkter Einhaltung der Wettbewerbsvorschriften und des Datenschutzrechts der Union eingerichtet werden.	Fähigkeit verbessert, Cyberbedrohungen angemessen zu bewerten, zu überwachen, abzuwehren und auf sie zu reagieren. Daher muss dafür gesorgt werden, dass auf Unionsebene Mechanismen für Vereinbarungen über den freiwilligen Informationsaustausch entstehen können. Zu diesem Zweck sollten die Mitgliedstaaten auch einschlägige Einrichtungen, die nicht unter diese Richtlinie fallen, aktiv unterstützen und dazu anhalten, sich an solchen Mechanismen zum Informationsaustausch zu beteiligen. ***Darüber hinaus könnten die Mitgliedstaaten auch die Möglichkeit prüfen, sich an gleichgesinnte Partnerländer zu wenden.*** Diese Mechanismen sollten unter uneingeschränkter Einhaltung der Wettbewerbsvorschriften und des Datenschutzrechts der Union eingerichtet werden. ***Die Mitgliedstaaten sollten zu diesem Zweck auch die zuständigen Behörden und CSIRTs dabei unterstützen, kostenlose oder zugängliche Unterstützungs-, Bildungs- und Prüfungsprogramme im Bereich Cybersicherheit für Einrichtungen anzubieten, die nicht in den Anwendungsbereich dieser Richtlinie fallen, insbesondere für Start-up-Unternehmen, KMU und Nichtregierungsorganisationen.***

Änderungsantrag 17

Vorschlag für eine Richtlinie
Erwägung 68 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(68a) Da die Cybersicherheit sowohl eine zivile als auch eine militärische Dimension hat, sollte auch der Austausch von Informationen zwischen verschiedenen Sektoren (Verteidigung, ziviler Sektor, Strafverfolgung und Außenpolitik) gefördert werden. Die

	Gemeinsame Cyber-Einheit könnte einen wichtigen Beitrag dazu leisten, die Union vor Cyberangriffen zu schützen, indem sie Akteure dabei unterstützt, ein gemeinsames Verständnis der Bedrohungslage zu gewinnen und ihre Reaktionen zu koordinieren.

Änderungsantrag 18

Vorschlag für eine Richtlinie
Erwägung 73

Vorschlag der Kommission	*Geänderter Text*
(73) Werden Geldbußen Unternehmen auferlegt, sollte zu diesem Zweck der Begriff „Unternehmen“ im Sinne der Artikel 101 und 102 AEUV verstanden werden. Werden Geldbußen Personen auferlegt, bei denen es sich nicht um Unternehmen handelt, so sollte die Aufsichtsbehörde bei der geeigneten Bemessung der Geldbuße dem allgemeinen Einkommensniveau in dem betreffenden Mitgliedstaat und der wirtschaftlichen Lage der Personen Rechnung tragen. Die Mitgliedstaaten sollten bestimmen können, ob und inwieweit gegen Behörden Geldbußen verhängt werden können. Auch wenn die zuständigen Behörden bereits Geldbußen auferlegt haben, können sie ihre anderen Befugnisse ausüben oder andere Sanktionen verhängen, die in den nationalen Vorschriften zur Umsetzung dieser Richtlinie festgelegt sind.	(73) Werden Geldbußen Unternehmen auferlegt, sollte zu diesem Zweck der Begriff „Unternehmen“ im Sinne der Artikel 101 und 102 AEUV verstanden werden. Werden Geldbußen Personen auferlegt, bei denen es sich nicht um Unternehmen handelt, so sollte die Aufsichtsbehörde bei der geeigneten Bemessung der Geldbuße ***unbeschadet der Ziele dieser Richtlinie*** dem allgemeinen Einkommensniveau in dem betreffenden Mitgliedstaat und der wirtschaftlichen Lage der Personen Rechnung tragen. Die Mitgliedstaaten sollten bestimmen können, ob und inwieweit gegen Behörden Geldbußen verhängt werden können. Auch wenn die zuständigen Behörden bereits Geldbußen auferlegt haben, können sie ihre anderen Befugnisse ausüben oder andere Sanktionen verhängen, die in den nationalen Vorschriften zur Umsetzung dieser Richtlinie festgelegt sind.

Änderungsantrag 19

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) ein Konzept für die Cybersicherheit in der Lieferkette für IKT-Produkte und -	a) ein Konzept für die Cybersicherheit in der Lieferkette für IKT-Produkte und -

Dienste, die von wesentlichen und wichtigen Einrichtungen für die Erbringung ihrer Dienste genutzt werden;	Dienste, die von wesentlichen und wichtigen Einrichtungen für die Erbringung ihrer Dienste genutzt werden***, auf der Grundlage einer umfassenden Bewertung der potenziellen Bedrohungen für Lieferketten***;

Änderungsantrag 20

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe b a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ba) eine Strategie zur Förderung der Interoperabilität und der Einhaltung gemeinsamer Standards der Union in Bezug auf die Cybersicherheit;

Änderungsantrag 21

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe d

Vorschlag der Kommission	*Geänderter Text*
d) ein Konzept im Zusammenhang mit der Aufrechterhaltung der allgemeinen Verfügbarkeit und Integrität des öffentlichen Kerns des offenen Internets;	d) ein Konzept im Zusammenhang mit der Aufrechterhaltung der allgemeinen Verfügbarkeit und Integrität des öffentlichen Kerns des offenen Internets***, gegebenenfalls einschließlich der Cybersicherheit von Unterseekommunikationskabeln***;

Änderungsantrag 22

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe f

Vorschlag der Kommission	*Geänderter Text*
f) ein Konzept zur Unterstützung von Hochschul- und Forschungseinrichtungen bei der Entwicklung von Cybersicherheitsinstrumenten und sicherer Netzinfrastruktur;	f) ein Konzept zur Unterstützung von Hochschul- und Forschungseinrichtungen bei der ***Forschung im Bereich der Cybersicherheit und bei der*** Entwicklung von Cybersicherheitsinstrumenten und

sicherer Netzinfrastruktur;

Änderungsantrag 23

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe h

Vorschlag der Kommission	*Geänderter Text*
h) ein Konzept, das auf die spezifischen Bedürfnisse von KMU – insbesondere vom Anwendungsbereich dieser Richtlinie ausgenommener ***KMU*** – ausgerichtet ist und Orientierungshilfen sowie Unterstützung bei der Verbesserung ihrer Resilienz gegenüber Cybersicherheitsbedrohungen bietet**.**	h) ein Konzept, das auf die spezifischen Bedürfnisse von ***Start-up-Unternehmen,*** KMU ***und Nichtregierungsorganisationen*** – insbesondere vom Anwendungsbereich dieser Richtlinie ausgenommener ***Unternehmen und Organisationen*** – ausgerichtet ist und Orientierungshilfen sowie Unterstützung bei der Verbesserung ihrer Resilienz gegenüber Cybersicherheitsbedrohungen***, bei der Reaktion auf Cybersicherheitsvorfälle und bei der Suche nach Unterstützung im Bereich der Cybersicherheit*** bietet***;***

Änderungsantrag 24

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe h a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ha) eine Strategie zur Förderung der Nutzung und Entwicklung quelloffener Software.

Änderungsantrag 25

Vorschlag für eine Richtlinie
Artikel 6 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Jeder Mitgliedstaat benennt eines seiner CSIRTs gemäß Artikel 9 als Koordinator für die Zwecke einer ***koordinierten*** Offenlegung von	(1) Jeder Mitgliedstaat benennt eines seiner CSIRTs gemäß Artikel 9 als Koordinator für die Zwecke einer ***verpflichtenden verantwortungsbewussten***

Schwachstellen. Das benannte CSIRT fungiert als vertrauenswürdiger Vermittler und erleichtert erforderlichenfalls die Interaktion zwischen der meldenden Einrichtung und dem Hersteller oder Anbieter von IKT-Produkten oder -Diensten. Betrifft die gemeldete Schwachstelle mehrere Hersteller oder Anbieter von IKT-Produkten oder -Diensten in der Union, so arbeitet das benannte CSIRT jedes betroffenen Mitgliedstaats mit dem CSIRT-Netzwerk zusammen.

Offenlegung von Schwachstellen. Das benannte CSIRT fungiert als vertrauenswürdiger Vermittler und erleichtert erforderlichenfalls die Interaktion zwischen der meldenden Einrichtung und dem Hersteller oder Anbieter von IKT-Produkten oder -Diensten. Betrifft die gemeldete Schwachstelle mehrere Hersteller oder Anbieter von IKT-Produkten oder -Diensten in der Union, so arbeitet das benannte CSIRT jedes betroffenen Mitgliedstaats mit dem CSIRT-Netzwerk zusammen.

Änderungsantrag 26

Vorschlag für eine Richtlinie
Artikel 6 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die ENISA entwickelt und pflegt ein europäisches Schwachstellenregister. Zu diesem Zweck führt die ENISA geeignete Informationssysteme, Konzepte und Verfahren ein und pflegt diese, damit insbesondere wichtige und wesentliche Einrichtungen sowie deren Anbieter von Netz- und Informationssystemen Schwachstellen in IKT-Produkten oder -Diensten offenlegen und registrieren können und allen interessierten Kreisen Zugang zu den im Register enthaltenen Informationen über Schwachstellen gewährt werden kann. Das Register muss insbesondere Folgendes umfassen: Informationen zur Beschreibung der Schwachstelle, des betroffenen IKT-Produkts oder der betroffenen IKT-Dienste sowie zum Ausmaß der Schwachstelle im Hinblick auf die Umstände, unter denen sie ausgenutzt werden kann, Informationen zur Verfügbarkeit entsprechender Patches und bei Nichtverfügbarkeit von Patches Orientierungshilfen für die Nutzer gefährdeter Produkte und Dienste, wie die von offengelegten Schwachstellen	(2) Die ENISA entwickelt und pflegt ein europäisches Schwachstellenregister. Zu diesem Zweck führt die ENISA geeignete Informationssysteme, Konzepte und Verfahren ein und pflegt diese, damit insbesondere wichtige und wesentliche Einrichtungen sowie deren Anbieter von Netz- und Informationssystemen Schwachstellen in IKT-Produkten oder -Diensten offenlegen und registrieren können und allen interessierten Kreisen Zugang zu den im Register enthaltenen Informationen über Schwachstellen gewährt werden kann. ***Gemäß Artikel 10 Absatz 2 erleichtern die CSIRTs Einrichtungen, die nicht in den Anwendungsbereich dieser Richtlinie fallen, insbesondere Start-up-Unternehmen, KMU und Nichtregierungsorganisationen, den Zugang zu Informationen über Schwachstellen, die im europäischen Schwachstellenregister erfasst sind, und unterstützen sie bei Risikominderungsmaßnahmen.*** Das Register muss insbesondere Folgendes

ausgehenden Risiken gemindert werden können.	umfassen: Informationen zur Beschreibung der Schwachstelle, des betroffenen IKT-Produkts oder der betroffenen IKT-Dienste sowie zum Ausmaß der Schwachstelle im Hinblick auf die Umstände, unter denen sie ausgenutzt werden kann, Informationen zur Verfügbarkeit entsprechender Patches und bei Nichtverfügbarkeit von Patches Orientierungshilfen für die Nutzer gefährdeter Produkte und Dienste, wie die von offengelegten Schwachstellen ausgehenden Risiken gemindert werden können.

Änderungsantrag 27

Vorschlag für eine Richtlinie
Artikel 7 – Absatz 3 – Buchstabe f

Vorschlag der Kommission	*Geänderter Text*
f) die zwischen den einschlägigen nationalen Behörden und Stellen vereinbarten nationalen Verfahren und Regelungen, die gewährleisten sollen, dass sich der Mitgliedstaat wirksam am koordinierten Management massiver Cybersicherheitsvorfälle und -krisen auf Unionsebene beteiligen und dieses unterstützen kann.	f) die zwischen den einschlägigen nationalen Behörden und Stellen vereinbarten nationalen Verfahren und Regelungen, die gewährleisten sollen, dass sich der Mitgliedstaat wirksam am koordinierten Management massiver Cybersicherheitsvorfälle und -krisen auf Unionsebene beteiligen und dieses unterstützen kann***, auch in Bezug auf Reaktionen auf einschlägige Anträge gemäß der Solidaritätsklausel***.

Änderungsantrag 28

Vorschlag für eine Richtlinie
Artikel 7 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
(4) Die Mitgliedstaaten teilen der Kommission ihre gemäß Absatz 1 benannten zuständigen Behörden innerhalb von drei Monaten nach der Benennung mit und übermitteln ihre nationalen Pläne für die Reaktion auf Cybersicherheitsvorfälle und -krisen gemäß Absatz 3 innerhalb von	(4) Die Mitgliedstaaten teilen der Kommission ihre gemäß Absatz 1 benannten zuständigen Behörden innerhalb von drei Monaten nach der Benennung mit und übermitteln ihre nationalen Pläne für die Reaktion auf Cybersicherheitsvorfälle und -krisen gemäß Absatz 3 innerhalb von

drei Monaten nach der Verabschiedung dieser Pläne. Die Mitgliedstaaten können bestimmte Informationen von ihrem Plan ausnehmen, wenn und soweit dies für ihre nationale Sicherheit unbedingt erforderlich ist.

drei Monaten nach der Verabschiedung dieser Pläne. Die Mitgliedstaaten können bestimmte Informationen von ihrem Plan ausnehmen, wenn und soweit dies für ihre nationale Sicherheit unbedingt erforderlich ist. ***Im Falle von Cybersicherheitsvorfällen und -krisen großen Ausmaßes, von denen mehr als ein Mitgliedstaat betroffen ist und die auf Ebene der Union von Bedeutung sind, sollte eine angemessene Krisenbewältigung und -steuerung eingerichtet werden. Diese Strukturen organisieren den Austausch von Informationen, die Koordinierung und Zusammenarbeit mit den Strukturen der Union im Bereich der äußeren Sicherheit und der militärischen Krisenbewältigung sowie den für die Sicherheit und Verteidigung zuständigen Stellen der Mitgliedstaaten.***

Änderungsantrag 29

Vorschlag für eine Richtlinie
Artikel 9 – Absatz 4 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(4a) Die CSIRTs arbeiten mit den für die Aufrechterhaltung der öffentlichen Sicherheit, die Verteidigung und nationale Sicherheit zuständigen nationalen Einrichtungen zusammen und tauschen einschlägige Informationen mit ihnen aus.

Änderungsantrag 30

Vorschlag für eine Richtlinie
Artikel 9 – Absatz 4 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	(4b) Die CSIRTs arbeiten in Bezug auf Cyberbedrohungen, Schwachstellen, bewährte Verfahren und Standards mit

vertrauenswürdigen Drittländern und internationalen Organisationen zusammen und tauschen unbeschadet des Unionsrechts, insbesondere der Verordnung (EU) 2016/679, einschlägige Informationen mit ihnen aus.

Änderungsantrag 31

Vorschlag für eine Richtlinie
Artikel 9 – Absatz 4 c (neu)

Vorschlag der Kommission	*Geänderter Text*
	(4c) Die CSIRTs stellen unbeschadet des Unionsrechts, insbesondere der Verordnung (EU) 2016/679, Unterstützung im Bereich der Cybersicherheit für CSIRTs oder entsprechende Strukturen in den Bewerberländern der Union und in anderen Drittländern des Westbalkans und der Östlichen Partnerschaft bereit.

Änderungsantrag 32

Vorschlag für eine Richtlinie
Artikel 10 – Absatz 2 – Buchstabe e a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ea) Bereitstellung von kostenlosen oder zugänglichen Unterstützungs-, Bildungs- und Prüfungsprogrammen im Bereich Cybersicherheit für Einrichtungen, die nicht in den Anwendungsbereich dieser Richtlinie fallen, insbesondere für Start-up-Unternehmen, KMU und Nichtregierungsorganisationen;

Änderungsantrag 33

Vorschlag für eine Richtlinie
Artikel 11 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
(4) Soweit dies zur wirksamen Wahrnehmung der in dieser Richtlinie festgelegten Aufgaben und Pflichten erforderlich ist, sorgen die Mitgliedstaaten für eine angemessene Zusammenarbeit zwischen den zuständigen Behörden und den zentralen Anlaufstellen sowie den Strafverfolgungsbehörden, den Datenschutzbehörden, den gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] für kritische Infrastrukturen zuständigen Behörden und den gemäß der Verordnung (EU) XXXX/XXXX des Europäischen Parlaments und des Rates [DORA-Verordnung][39] in dem jeweiligen Mitgliedstaat benannten nationalen Finanzbehörden.	(4) Soweit dies zur wirksamen Wahrnehmung der in dieser Richtlinie festgelegten Aufgaben und Pflichten erforderlich ist, sorgen die Mitgliedstaaten für eine angemessene Zusammenarbeit zwischen den zuständigen Behörden und den zentralen Anlaufstellen sowie den Strafverfolgungsbehörden, den Datenschutzbehörden, ***den nationalen Aufsichtsbehörden für künstliche Intelligenz, den für Daten-Governance zuständigen nationalen Behörden,*** den gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] für kritische Infrastrukturen zuständigen Behörden und den gemäß der Verordnung (EU) XXXX/XXXX des Europäischen Parlaments und des Rates [DORA-Verordnung][39] in dem jeweiligen Mitgliedstaat benannten nationalen Finanzbehörden.
[39] [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].	[39] [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].

Änderungsantrag 34

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 3 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(3) Die Kooperationsgruppe setzt sich aus Vertretern der Mitgliedstaaten, der Kommission ***und*** der ENISA zusammen. Der Europäische Auswärtige Dienst nimmt an den Tätigkeiten der Kooperationsgruppe als Beobachter teil. Die Europäischen Aufsichtsbehörden (ESAs) ***können*** sich gemäß Artikel 17 Absatz 5 Buchstabe c der Verordnung (EU) XXXX/XXXX [DORA-Verordnung] an den Tätigkeiten der Kooperationsgruppe ***beteiligen***.	(3) Die Kooperationsgruppe setzt sich aus Vertretern der Mitgliedstaaten, der Kommission***, von EU-CyCLONe,*** der ENISA ***und der Europäischen Verteidigungsagentur*** zusammen. Der Europäische Auswärtige Dienst nimmt an den Tätigkeiten der Kooperationsgruppe als Beobachter teil. Die ***nationalen Aufsichtsbehörden für künstliche Intelligenz, die für Daten-Governance zuständigen nationalen Behörden und die*** Europäischen Aufsichtsbehörden (ESAs) ***beteiligen*** sich gemäß Artikel 17 Absatz 5

	Buchstabe c der Verordnung (EU) XXXX/XXXX [DORA-Verordnung] an den Tätigkeiten der Kooperationsgruppe.

Änderungsantrag 35

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 4 – Buchstabe e a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ea) Zusammenarbeit, gegenseitige Unterstützung und Austausch von bewährten Verfahren und Informationen, unbeschadet des Unionsrechts, mit vertrauenswürdigen Drittländern und internationalen Organisationen;

Änderungsantrag 36

Vorschlag für eine Richtlinie
Artikel 13 – Absatz 3 – Buchstabe k

Vorschlag der Kommission	*Geänderter Text*
k) Zusammenarbeit und Informationsaustausch mit regionalen und unionsweiten Sicherheitseinsatzzentren, um die gemeinsame Lageerfassung bei Sicherheitsvorfällen und Bedrohungen in der gesamten Union zu verbessern;	k) Zusammenarbeit und Informationsaustausch mit regionalen und unionsweiten Sicherheitseinsatzzentren ***und gegebenenfalls mit militärischen CERTs***, um die gemeinsame Lageerfassung bei Sicherheitsvorfällen und Bedrohungen in der gesamten Union zu verbessern;

Änderungsantrag 37

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) EU-CyCLONe setzt sich aus den Vertretern der gemäß Artikel 7 benannten für das Krisenmanagement zuständigen Behörden der Mitgliedstaaten, der	(2) EU-CyCLONe setzt sich aus den Vertretern der gemäß Artikel 7 benannten für das Krisenmanagement zuständigen Behörden der Mitgliedstaaten, der

Kommission und der ENISA zusammen. ENISA führt die Sekretariatsgeschäfte des Netzwerks und unterstützt den sicheren Informationsaustausch.	Kommission***, des EAD*** und der ENISA zusammen. ENISA führt die Sekretariatsgeschäfte des Netzwerks und unterstützt den sicheren Informationsaustausch. ***Die für das Krisenmanagement zuständigen nationalen Behörden erhalten Beratung von einer zivilgesellschaftlichen Beratungsgruppe. Für Cybersicherheitsvorfälle und -krisen großen Ausmaßes auf Unionsebene, von denen mehr als ein Mitgliedstaat betroffen ist, wird eine Krisenmanagementstruktur auf Unionsebene unter Beteiligung aller einschlägigen Akteure eingerichtet. Diese Struktur umfasst die Gemeinsame Cyber-Einheit, CSIRTs, das CSIRT-Netzwerk, die Koordinierungsgruppe, die Kommission, den EAD und die ENISA. Von ihr wird auch die Geltendmachung und Anwendung der Solidaritätsklausel vorbereitet und umgesetzt.***

Änderungsantrag 38

Vorschlag für eine Richtlinie
Artikel 14 – Absatz 3 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) Verbesserung der Vorsorge im Hinblick auf das Management massiver Sicherheitsvorfälle und Krisen;	a) Verbesserung der Vorsorge im Hinblick auf das Management massiver Sicherheitsvorfälle und Krisen ***und Zusammenarbeit mit den für die Staatssicherheit und territoriale Verteidigung zuständigen Stellen der Mitgliedstaaten***;

Änderungsantrag 39

Vorschlag für eine Richtlinie
Artikel 17 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Mitgliedstaaten stellen sicher,	(2) Die Mitgliedstaaten stellen sicher,

dass die Mitglieder der Leitungsorgane regelmäßig an spezifischen Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf den Betrieb der Einrichtung zu erwerben.	dass die Mitglieder der Leitungsorgane regelmäßig an spezifischen Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf den Betrieb der Einrichtung zu erwerben. ***Die Mitgliedstaaten fordern die wesentlichen und wichtigen Einrichtungen auf, die Mitglieder der in Absatz 1 genannten Leitungsorgane regelmäßig hinsichtlich ihrer Eignung zu bewerten, die Einhaltung von Artikel 18 sicherzustellen.***

Änderungsantrag 40

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Die Mitgliedstaaten stellen sicher, dass die Einrichtungen bei der Erwägung geeigneter Maßnahmen nach Absatz 2 Buchstabe d die spezifischen Schwachstellen der einzelnen Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, berücksichtigen.	(3) Die Mitgliedstaaten stellen sicher, dass die Einrichtungen bei der Erwägung geeigneter Maßnahmen nach Absatz 2 Buchstabe d die spezifischen Schwachstellen der einzelnen Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse ***im Einklang mit den Cybersicherheitsstandards und -vorschriften der Union und potenzieller nichttechnischer Risikofaktoren, etwa versteckter Schwachstellen oder Hintertüren sowie potenzieller systemischer Versorgungsunterbrechungen,*** berücksichtigen.

Änderungsantrag 41

Vorschlag für eine Richtlinie
Artikel 19 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Die Kooperationsgruppe kann in Zusammenarbeit mit der Kommission und ***der ENISA*** koordinierte Risikobewertungen in Bezug auf die Sicherheit der Lieferketten bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte unter Berücksichtigung technischer und erforderlichenfalls nichttechnischer Risikofaktoren durchführen.	(1) Die Kooperationsgruppe kann in Zusammenarbeit mit der Kommission***,*** der ENISA ***und dem Europäischen Auswärtigen Dienst*** koordinierte Risikobewertungen in Bezug auf die Sicherheit der Lieferketten bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte unter Berücksichtigung technischer und erforderlichenfalls nichttechnischer Risikofaktoren durchführen.

Änderungsantrag 42

Vorschlag für eine Richtlinie
Artikel 19 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Kommission legt nach Konsultation der Kooperationsgruppe ***und*** der ENISA fest, welche spezifischen kritischen IKT-Dienste, -Systeme oder -Produkte der koordinierten Risikobewertung nach Absatz 1 unterzogen werden können.	(2) Die Kommission legt nach Konsultation der Kooperationsgruppe***,*** der ENISA ***und des Europäischen Auswärtigen Dienstes*** fest, welche spezifischen kritischen IKT-Dienste, -Systeme oder -Produkte der koordinierten Risikobewertung nach Absatz 1 unterzogen werden können.

Änderungsantrag 43

Vorschlag für eine Richtlinie
Artikel 19 – Absatz 2 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(2a) Werden Risiken für spezifische kritische IKT-Dienste, Systeme oder Produktionsversorgungsketten festgestellt, gibt die Kommission nach Konsultation der Kooperationsgruppe, der ENISA und des Europäischen Auswärtigen Dienstes Empfehlungen an die Mitgliedstaaten und die in dieser Verordnung festgelegten zuständigen nationalen Behörden ab, um

	die festgestellten Risiken zu beseitigen und die Resilienz gegenüber diesen Risiken zu erhöhen.

Änderungsantrag 44

Vorschlag für eine Richtlinie
Artikel 25 – Absatz 1 – Buchstabe c a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ca) Informationen über das Leitungsorgan, das im Einklang mit Artikel 17 für die in Artikel 18 festgelegten Risikomanagementmaßnahmen im Bereich der Cybersicherheit zuständig ist;

Änderungsantrag 45

Vorschlag für eine Richtlinie
Artikel 29 – Absatz 2 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) gezielte Sicherheitsprüfungen auf der Grundlage von Risikobewertungen oder verfügbaren risikobezogenen Informationen;	c) gezielte Sicherheitsprüfungen auf der Grundlage von Risikobewertungen oder verfügbaren risikobezogenen Informationen***, auch in Bezug auf Risiken in Verbindung mit Lieferketten gemäß Artikel 18 Absatz 3***;

Änderungsantrag 46

Vorschlag für eine Richtlinie
Artikel 30 – Absatz 2 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) gezielte Sicherheitsprüfungen auf der Grundlage von Risikobewertungen oder verfügbaren risikobezogenen Informationen;	b) gezielte Sicherheitsprüfungen auf der Grundlage von Risikobewertungen oder verfügbaren risikobezogenen Informationen***, auch in Bezug auf Risiken in Verbindung mit Lieferketten gemäß Artikel 18 Absatz 3***;

Änderungsantrag 47

Vorschlag für eine Richtlinie
Anhang I – WESENTLICHE EINRICHTUNGEN: SEKTOREN, TEILSEKTOREN UND ARTEN VON EINRICHTUNGEN – Sektor 6 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	6a. Bildung und Forschung – Hochschul- und Forschungseinrichtungen

Änderungsantrag 48

Vorschlag für eine Richtlinie
Anhang I – WESENTLICHE EINRICHTUNGEN: SEKTOREN, TEILSEKTOREN UND ARTEN VON EINRICHTUNGEN – Sektor 9 Öffentliche Verwaltung – Art der Einrichtung

Vorschlag der Kommission	*Geänderter Text*
– Einrichtungen der öffentlichen Verwaltung von Zentralregierungen	– Einrichtungen der öffentlichen Verwaltung von Zentralregierungen
– Einrichtungen der öffentlichen Verwaltung der in Anhang I der Verordnung (EG) Nr. 1059/2003[27] aufgeführten Regionen der NUTS-Ebene 1	– Einrichtungen der öffentlichen Verwaltung der in Anhang I der Verordnung (EG) Nr. 1059/2003[27] aufgeführten Regionen der NUTS-Ebene 1***[27a (neu)]***
– Einrichtungen der öffentlichen Verwaltung der in Anhang I der Verordnung (EG) Nr. 1059/2003 aufgeführten Regionen der NUTS-Ebene 2	– Einrichtungen der öffentlichen Verwaltung der in Anhang I der Verordnung (EG) Nr. 1059/2003 aufgeführten Regionen der NUTS-Ebene 2***[27b (neu)]***
[27] Verordnung (EG) Nr. 1059/2003 des Europäischen Parlaments und des Rates vom 26. Mai 2003 über die Schaffung einer gemeinsamen Klassifikation der Gebietseinheiten für die Statistik (NUTS) (ABl. L 154 vom 21.6.2003, S. 1).	[27] Verordnung (EG) Nr. 1059/2003 des Europäischen Parlaments und des Rates vom 26. Mai 2003 über die Schaffung einer gemeinsamen Klassifikation der Gebietseinheiten für die Statistik (NUTS) (ABl. L 154 vom 21.6.2003, S. 1).
	[27a (neu)] Oder der entsprechenden Verwaltungseinheiten in Mitgliedstaaten, in denen sich die NUTS-Klassifikation

noch nicht in den institutionellen Verwaltungsstrukturen widerspiegelt.

27b (neu) Oder der entsprechenden Verwaltungseinheiten in Mitgliedstaaten, in denen sich die NUTS-Klassifikation noch nicht in den institutionellen Verwaltungsstrukturen widerspiegelt.

VERFAHREN DES MITBERATENDEN AUSSCHUSSES

Titel	Maßnahmen zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus in der Union, Aufhebung der Richtlinie (EU) 2016/1148
Bezugsdokumente – Verfahrensnummer	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Federführender Ausschuss Datum der Bekanntgabe im Plenum	ITRE 21.1.2021
Stellungnahme von Datum der Bekanntgabe im Plenum	AFET 21.1.2021
Verfasser(in) der Stellungnahme Datum der Benennung	Markéta Gregorová 22.2.2021
Prüfung im Ausschuss	25.5.2021 16.6.2021 17.6.2021
Datum der Annahme	14.7.2021
Ergebnis der Schlussabstimmung	+: 59 –: 5 0: 6
Zum Zeitpunkt der Schlussabstimmung anwesende Mitglieder	Alviina Alametsä, Alexander Alexandrov Yordanov, Maria Arena, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Reinhard Bütikofer, Fabio Massimo Castaldo, Susanna Ceccardi, Włodzimierz Cimoszewicz, Katalin Cseh, Tanja Fajon, Anna Fotyga, Michael Gahler, Giorgos Georgiou, Sunčana Glavak, Raphaël Glucksmann, Klemen Grošelj, Bernard Guetta, Márton Gyöngyösi, Andrzej Halicki, Sandra Kalniete, Dietmar Köster, Maximilian Krah, Andrius Kubilius, Ilhan Kyuchyuk, David Lega, Miriam Lexmann, Nathalie Loiseau, Antonio López-Istúriz White, Jaak Madison, Claudiu Manda, Thierry Mariani, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Javier Nart, Urmas Paet, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Manu Pineda, Giuliano Pisapia, Thijs Reuten, Jérôme Rivière, María Soraya Rodríguez Ramos, Nacho Sánchez Amor, Isabel Santos, Jacek Saryusz-Wolski, Andreas Schieder, Radosław Sikorski, Jordi Solé, Sergei Stanishev, Tineke Strik, Hermann Tertsch, Hilde Vautmans, Harald Vilimsky, Idoia Villanueva Ruiz, Viola Von Cramon-Taubadel, Thomas Waitz, Witold Jan Waszczykowski, Charlie Weimers, Isabel Wiseler-Lima, Salima Yenbou, Željana Zovko
Zum Zeitpunkt der Schlussabstimmung anwesende Stellvertreter	Ioan-Rareş Bogdan, Andrey Kovatchev, Marisa Matias, Gabriel Mato, Milan Zver

NAMENTLICHE SCHLUSSABSTIMMUNG IM MITBERATENDEN AUSSCHUSS

59	+
ECR	Anna Fotyga, Jacek Saryusz-Wolski, Hermann Tertsch, Witold Jan Waszczykowski
ID	Anna Bonfrisco, Susanna Ceccardi
NI	Fabio Massimo Castaldo, Márton Gyöngyösi
PPE	Alexander Alexandrov Yordanov, Traian Băsescu, Ioan-Rareş Bogdan, Michael Gahler, Sunčana Glavak, Andrzej Halicki, Sandra Kalniete, Andrey Kovatchev, Andrius Kubilius, David Lega, Miriam Lexmann, Antonio López-Istúriz White, Gabriel Mato, Vangelis Meimarakis, Francisco José Millán Mon, Radosław Sikorski, Isabel Wiseler-Lima, Željana Zovko, Milan Zver
Renew	Petras Auštrevičius, Katalin Cseh, Klemen Grošelj, Bernard Guetta, Ilhan Kyuchyuk, Nathalie Loiseau, Javier Nart, Urmas Paet, María Soraya Rodríguez Ramos, Hilde Vautmans
S&D	Maria Arena, Włodzimierz Cimoszewicz, Tanja Fajon, Raphaël Glucksmann, Dietmar Köster, Claudiu Manda, Sven Mikser, Demetris Papadakis, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Isabel Santos, Andreas Schieder, Sergei Stanishev
Verts/ALE	Alviina Alametsä, Reinhard Bütikofer, Jordi Solé, Tineke Strik, Viola Von Cramon-Taubadel, Thomas Waitz, Salima Yenbou

5	-
NI	Kostas Papadakis
The Left	Giorgos Georgiou, Marisa Matias, Manu Pineda, Idoia Villanueva Ruiz

6	0
ECR	Charlie Weimers
ID	Maximilian Krah, Jaak Madison, Thierry Mariani, Jérôme Rivière, Harald Vilimsky

Erklärung der benutzten Zeichen:
+ : dafür
- : dagegen
0 : Enthaltung

14.7.2021

STELLUNGNAHME DES AUSSCHUSSES FÜR BINNENMARKT UND VERBRAUCHERSCHUTZ

für den Ausschuss für Industrie, Forschung und Energie

zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Verfasser der Stellungnahme: Morten Løkkegaard

KURZE BEGRÜNDUNG

Im Allgemeinen begrüßt der Verfasser den Legislativvorschlag für eine Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (im Folgenden: „NIS-2-Richtlinie“). Der Verfasser ist der Ansicht, dass die Online-Sicherheit in einer zunehmend digitalisierten Welt von entscheidender Bedeutung für die Sicherstellung eines sicheren digitalen Umfelds sowie für das Funktionieren des Binnenmarkts ist, in dem Verbraucher und Wirtschaftsakteure frei agieren können.

Der Vorschlag für die NIS-2-Richtlinie ist eine deutliche Verbesserung gegenüber der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (im Folgenden: „NIS-1-Richtlinie“). In ihm werden die wichtigsten Mängel der NIS-1-Richtlinie aufgezählt. Hierzu gehören beispielsweise das niedrige Cyberresilienzniveau bei Unternehmen und Branchen sowie die unterschiedliche Resilienz und die schwach ausgeprägte gemeinsame Lageerfassung und Krisenreaktion in und zwischen den Mitgliedstaaten. Der Verfasser begrüßt die Bestrebungen, dies mit der NIS-2-Richtlinie zu beheben.

Anwendungsbereich

Der Verfasser begrüßt den erweiterten Anwendungsbereich des Vorschlags für die NIS-2-Richtlinie, insbesondere die Einbeziehung neuer Bereiche wie der öffentlichen Verwaltung. Durch die klare Liste der einbezogenen Sektoren und Dienste wird der Ermessensspielraum der Mitgliedstaaten bei der Festlegung der konkreten Einrichtungen, die der Richtlinie unterliegen, sicherlich verringert und somit die Fragmentierung des Binnenmarktes reduziert.

Im Hinblick auf die berücksichtigten Sektoren und Dienste hat die Kommission einen Schwellenwert für die Größe als einheitliches Kriterium vorgeschlagen, um festzulegen, welche

Einrichtungen in den Anwendungsbereich der Richtlinie fallen. Dieses Kriterium bietet zweifellos den Vorteil, dass für Rechtssicherheit gesorgt wird und gleichzeitig die Unterschiede zwischen den Mitgliedstaaten abgebaut werden.

Der Verfasser begrüßt zwar den erweiterten sektorbezogenen Anwendungsbereich, ist aber der Ansicht, dass dieses allgemeine Kriterium mit einer Bewertung der Kritikalität von Einrichtungen in den einzelnen Sektoren kombiniert werden sollte. Dies würde erlauben, mittlere und große Einrichtungen, die nach einer Risikobewertung als Einrichtungen von geringer Kritikalität und mit geringer Abhängigkeit von anderweitig kritischen Einrichtungen gelten, aus dem Anwendungsbereich der Richtlinie auszunehmen.

Der Verfasser betont jedoch, dass dies nicht als Möglichkeit für abweichende Auslegungen der Mitgliedstaaten angesehen werden sollte. Um sicherzustellen, dass dadurch nicht zu einer fragmentierten Umsetzung in den Mitgliedstaaten beigetragen wird, wird die Kommission aufgefordert, hierzu klare Orientierungshilfen zu geben.

Schließlich begrüßt der Verfasser zwar den Ausschluss von Kleinstunternehmen und kleinen Unternehmen aus dem Anwendungsbereich, aber er ist der Auffassung, dass deren freiwillige Einbeziehung gefördert werden muss, da auch Kleinst- und Kleineinrichtungen Cyberangriffen ausgesetzt und von ihnen betroffen sind.

Koordinierte Rechtsrahmen für die Cybersicherheit

Der Verfasser begrüßt das Kapitel, in dem verschiedene Elemente der nationalen Cybersicherheitsstrategien und ihrer Krisenmanagementinstrumente festgelegt werden. Es wird vorgeschlagen, dass die Mitgliedstaaten im Rahmen ihrer nationalen Cybersicherheitsstrategien eine Politik zur Förderung des Einsatzes von Kryptografie und Verschlüsselung, insbesondere durch KMU, verfolgen.

Der Verfasser begrüßt die Entwicklung eines europäischen Schwachstellenregisters durch die ENISA, ist jedoch der Ansicht, dass es wichtig ist, bei der Registrierung Betriebs- und Geschäftsgeheimnisse zu achten und die Einrichtungen nicht unnötig zu belasten.

Zusammenarbeit zwischen den Mitgliedstaaten

Der Verfasser begrüßt insbesondere die in der NIS-2-Richtlinie vorgesehene strukturiertere Zusammenarbeit zwischen den Mitgliedstaaten innerhalb der Kooperationsgruppe, des CSIRT-Netzwerks und der neu geschaffenen Gruppe für große Cybersicherheitsvorfälle. Es muss jedoch sichergestellt werden, dass das Vertrauen zwischen den Mitgliedstaaten und ihre Bereitschaft, Informationen auszutauschen, gestärkt werden, denn die Wirksamkeit der Zusammenarbeit ist bei der Sicherstellung eines hohen Cybersicherheitsniveaus in der EU von großer Bedeutung.

Vor dem Hintergrund dieses Standpunkts wurde eine Reihe von Änderungsanträgen ausgearbeitet, um die Rolle der Netzwerke zu stärken. Insbesondere hält der Verfasser Peer Reviews für einen fruchtbaren Weg, um das Vertrauen der Mitgliedstaaten ineinander zu stärken, und er spricht sich dafür aus, dass ihnen bei der Bewertung der Wirksamkeit der Cybersicherheitskonzepte der einzelnen Mitgliedstaaten eine entscheidende Rolle zukommt.

Cybersicherheitsrisikomanagement

Die Ausweitung der Risikobewertung auf die gesamte Lieferkette (Artikel 18 und 19) wird begrüßt, doch der Verfasser betont, dass diesbezüglich Klarstellungen nötig sind, um den von dieser Anforderung betroffenen Einrichtungen und den Mitgliedstaaten bei der Durchführung einer koordinierten Risikobewertung in Bezug auf die Sicherheit besonders kritischer Sektoren oder Lieferketten klare Orientierungshilfen zu geben.

Meldepflichten

Der Verfasser ist der Auffassung, dass in Bezug auf bestimmte Punkte der überarbeiteten Richtlinie mehr Klarheit geschaffen werden sollte, hauptsächlich hinsichtlich einiger Verpflichtungen für Unternehmen, die in den Anwendungsbereich der NIS-2-Richtlinie fallen. Der Verfasser hat sich unter Berücksichtigung des Endziels der wirksamen Umsetzung der Richtlinie darum bemüht, die Verwaltungslast zu verringern und es Unternehmen zu erleichtern, die neuen Vorschriften einzuhalten.

Der Vorschlag des Verfassers besteht darin, die vorgeschlagene Frist von 24 Stunden in Bezug auf die Meldepflichten für die erste Meldung auf 72 Stunden zu verlängern, um es Unternehmen zu ermöglichen, vor der Meldung wirksam gegen laufende Cyberangriffe vorzugehen. Darüber hinaus wird vorgeschlagen, jegliche Bezugnahme auf eine Pflichtmeldung sogenannter „potenzieller Vorfälle“ zu streichen.

ÄNDERUNGSANTRÄGE

Der Ausschuss für Binnenmarkt und Verbraucherschutz ersucht den federführenden Ausschuss für Industrie, Forschung und Energie, folgende Änderungsanträge zu berücksichtigen:

Änderungsantrag 1
Vorschlag für eine Richtlinie
Erwägung 5

Vorschlag der Kommission	*Geänderter Text*
(5) All diese Unterschiede führen zu einer Fragmentierung des Binnenmarkts und können sich nachteilig auf dessen Funktionieren auswirken und aufgrund der Anwendung unterschiedlicher Normen insbesondere die grenzüberschreitende Erbringung von Diensten und das Niveau der Cyberresilienz beeinträchtigen. Ziel der vorliegenden Richtlinie ist, diese großen Unterschiede zwischen den Mitgliedstaaten zu beseitigen, indem insbesondere Mindestvorschriften für einen funktionierenden und koordinierten Rechtsrahmen festgelegt werden,	(5) All diese Unterschiede führen zu einer Fragmentierung des Binnenmarkts und können sich nachteilig auf dessen Funktionieren auswirken und aufgrund der Anwendung unterschiedlicher Normen insbesondere die grenzüberschreitende Erbringung von Diensten und das Niveau der Cyberresilienz beeinträchtigen. Ziel der vorliegenden Richtlinie ist, diese großen Unterschiede zwischen den Mitgliedstaaten zu beseitigen ***und den Binnenmarkt zu stärken***, indem insbesondere Mindestvorschriften für einen funktionierenden und koordinierten

Mechanismen für die wirksame Zusammenarbeit zwischen den zuständigen Behörden in den einzelnen Mitgliedstaaten vorgesehen werden, die Liste der Sektoren und Tätigkeiten, die Pflichten im Hinblick auf die Cybersicherheit unterliegen, aktualisiert wird und wirksame Abhilfemaßnahmen und Sanktionen, die für die wirksame Durchsetzung dieser Verpflichtungen von entscheidender Bedeutung sind, eingeführt werden. Daher sollte die Richtlinie (EU) 2016/1148 aufgehoben und durch die vorliegende Richtlinie ersetzt werden.	Rechtsrahmen festgelegt werden, Mechanismen für die wirksame Zusammenarbeit zwischen den zuständigen Behörden in den einzelnen Mitgliedstaaten vorgesehen werden, die Liste der Sektoren und Tätigkeiten, die Pflichten im Hinblick auf die Cybersicherheit unterliegen, aktualisiert wird und wirksame Abhilfemaßnahmen und Sanktionen, die für die wirksame Durchsetzung dieser Verpflichtungen von entscheidender Bedeutung sind, eingeführt werden. Daher sollte die Richtlinie (EU) 2016/1148 aufgehoben und durch die vorliegende Richtlinie ersetzt werden.

Änderungsantrag 2
Vorschlag für eine Richtlinie
Erwägung 6 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(6a) Die Richtlinie berührt nicht die im Unionsrecht festgelegten Vorschriften über den Schutz personenbezogener Daten.

Änderungsantrag 3
Vorschlag für eine Richtlinie
Erwägung 9

Vorschlag der Kommission	*Geänderter Text*
(9) Allerdings sollten auch Klein- und Kleinsteinrichtungen, die bestimmte Kriterien erfüllen, nach denen sie eine Schlüsselrolle für die Wirtschaft oder Gesellschaft des betreffenden Mitgliedstaats oder für bestimmte Sektoren oder Arten von Diensten spielen, von der vorliegenden Richtlinie erfasst werden. Die Mitgliedstaaten sollten für die Erstellung einer Liste solcher Einrichtungen zuständig sein und diese der Kommission übermitteln.	(9) Allerdings sollten auch Klein- und Kleinsteinrichtungen, die bestimmte Kriterien erfüllen, nach denen sie eine Schlüsselrolle für die Wirtschaft oder Gesellschaft des betreffenden Mitgliedstaats oder für bestimmte Sektoren oder Arten von Diensten spielen, von der vorliegenden Richtlinie erfasst werden. Die Mitgliedstaaten sollten für die Erstellung einer Liste solcher Einrichtungen zuständig sein und diese der Kommission übermitteln. ***Die Kommission sollte klare Orientierungshilfen zu den Kriterien***

	geben, anhand derer bestimmt wird, welche Klein- und Kleinsteinrichtungen wesentlich oder wichtig sind, insbesondere, wenn Dienste in mehreren Mitgliedstaaten erbracht werden.

Änderungsantrag 4
Vorschlag für eine Richtlinie
Erwägung 10

Vorschlag der Kommission	*Geänderter Text*
(10) Die Kommission ***kann*** in Zusammenarbeit mit der Kooperationsgruppe Leitlinien für die Anwendung der für Klein- und Kleinstunternehmen geltenden Kriterien herausgeben.	(10) Die Kommission ***sollte*** in Zusammenarbeit mit der Kooperationsgruppe Leitlinien für die Anwendung der für Klein- und Kleinstunternehmen geltenden Kriterien herausgeben.

Änderungsantrag 5
Vorschlag für eine Richtlinie
Erwägung 12 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(12a) Die Ausweitung des Anwendungsbereichs dieser Richtlinie bringt die Einbeziehung von Einrichtungen mit sich, die sektorspezifischen Vorschriften unterliegen. Um Doppelregulierungen und Belastungen vorzubeugen, sollte die Kommission sicherstellen, dass sektorspezifische Rechtsakte, gemäß denen wesentliche oder wichtige Einrichtungen entweder Risikomanagementmaßnahmen im Bereich der Cybersicherheit ergreifen oder Sicherheitsvorfälle oder erhebliche Cyberbedrohungen melden müssen, mit dieser Richtlinie im Einklang stehen.

Änderungsantrag 6
Vorschlag für eine Richtlinie
Erwägung 12 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	(12b) Die Kommission sollte klare Leitlinien zu dieser Richtlinie veröffentlichen, um dazu beizutragen, die Harmonisierung der Umsetzung in den Mitgliedstaaten sicherzustellen und eine Fragmentierung zu verhindern.

Änderungsantrag 7
Vorschlag für eine Richtlinie
Erwägung 12 c (neu)

Vorschlag der Kommission	*Geänderter Text*
	(12c) Die Kommission sollte ferner Leitlinien herausgeben, um die Mitgliedstaaten bei der korrekten Umsetzung der Bestimmungen über den Anwendungsbereich zu unterstützen und die Verhältnismäßigkeit der in dieser Richtlinie dargelegten Pflichten unter Berücksichtigung der Kritikalität in den Anwendungsbereich fallender Einrichtungen zu evaluieren, insbesondere, wenn sie auf Einrichtungen mit komplexen Geschäftsmodellen oder Betriebsumgebungen Anwendung finden, wobei eine Einrichtung gleichzeitig die Kriterien für wesentliche und für wichtige Einrichtungen erfüllen kann oder gleichzeitig Tätigkeiten, die in den Anwendungsbereich dieser Richtlinie fallen, und andere Tätigkeiten ausführen kann. Wenn die Haupttätigkeit von Einrichtungen nicht in den Anwendungsbereich dieser Richtlinie fällt, aber eine Nebentätigkeit in ihren Anwendungsbereich fällt, so sollten die Bestimmungen nur für die Funktions- oder Abteilungsebene in einer Einrichtung gelten, die in den Anwendungsbereich dieser Richtlinie fällt.

Änderungsantrag 8
Vorschlag für eine Richtlinie
Erwägung 14

Vorschlag der Kommission	*Geänderter Text*
(14) Angesichts der Zusammenhänge zwischen der Cybersicherheit und der physischen Sicherheit von Einrichtungen sollte dafür gesorgt werden, dass der Ansatz der Richtlinie (EU) XXX/XXX des Europäischen Parlaments und des Rates[17] und der Ansatz der vorliegenden Richtlinie kohärent sind. Um dies zu erreichen, sollten die Mitgliedstaaten sicherstellen, dass kritische Einrichtungen und diesen gleichgestellte Einrichtungen im Sinne der Richtlinie (EU) XXX/XXX als wesentliche Einrichtungen im Sinne der vorliegenden Richtlinie gelten. Die Mitgliedstaaten sollten auch sicherstellen, dass ihre Cybersicherheitsstrategien einen politischen Rahmen für eine verstärkte Koordinierung zwischen der gemäß der vorliegenden Richtlinie zuständigen Behörde und der gemäß Richtlinie (EU) XXX/XXX zuständigen Behörde beim Informationsaustausch über Sicherheitsvorfälle und Cyberbedrohungen und bei der Wahrnehmung von Aufsichtsaufgaben vorsehen. Die gemäß diesen beiden Richtlinien zuständigen Behörden sollten zusammenarbeiten und Informationen austauschen, insbesondere in Bezug auf die Ermittlung kritischer Einrichtungen, Cyberbedrohungen, Cybersicherheitsrisiken und Sicherheitsvorfälle, die kritische Einrichtungen beeinträchtigen, sowie über die von kritischen Einrichtungen ergriffenen Cybersicherheitsmaßnahmen. Auf Ersuchen der gemäß der Richtlinie (EU) XXX/XXX zuständigen Behörden sollte den gemäß der vorliegenden Richtlinie zuständigen Behörden gestattet werden, ihre Aufsichts- und Durchsetzungsbefugnisse gegenüber einer als kritisch eingestuften wesentlichen Einrichtung auszuüben. Beide Behörden	(14) Angesichts der Zusammenhänge zwischen der Cybersicherheit und der physischen Sicherheit von Einrichtungen sollte dafür gesorgt werden, dass der Ansatz der Richtlinie (EU) XXX/XXX des Europäischen Parlaments und des Rates[17] und der Ansatz der vorliegenden Richtlinie kohärent sind. Um dies zu erreichen, sollten die Mitgliedstaaten sicherstellen, dass kritische Einrichtungen und diesen gleichgestellte Einrichtungen im Sinne der Richtlinie (EU) XXX/XXX als wesentliche Einrichtungen im Sinne der vorliegenden Richtlinie gelten. Die Mitgliedstaaten sollten auch sicherstellen, dass ihre ***nationalen*** Cybersicherheitsstrategien einen politischen Rahmen für eine verstärkte Koordinierung zwischen der gemäß der vorliegenden Richtlinie zuständigen Behörde und der gemäß ***der*** Richtlinie (EU) XXX/XXX zuständigen Behörde ***bei der Meldung von Sicherheitsvorfällen,*** beim Informationsaustausch über Sicherheitsvorfälle***, Beinahe-Vorfälle*** und Cyberbedrohungen und bei der Wahrnehmung von Aufsichtsaufgaben vorsehen. Die gemäß diesen beiden Richtlinien zuständigen Behörden sollten zusammenarbeiten und Informationen austauschen, insbesondere in Bezug auf die Ermittlung kritischer Einrichtungen, Cyberbedrohungen, Cybersicherheitsrisiken und Sicherheitsvorfälle, die kritische Einrichtungen beeinträchtigen, sowie über die von kritischen Einrichtungen ergriffenen Cybersicherheitsmaßnahmen. Auf Ersuchen der gemäß der Richtlinie (EU) XXX/XXX zuständigen Behörden sollte den gemäß der vorliegenden Richtlinie zuständigen Behörden gestattet werden, ihre Aufsichts- und

sollten zu diesem Zweck zusammenarbeiten und Informationen austauschen.

Durchsetzungsbefugnisse gegenüber einer als kritisch eingestuften wesentlichen Einrichtung auszuüben. Beide Behörden sollten zu diesem Zweck zusammenarbeiten und Informationen austauschen.

---

[17] [vollständigen Titel und Fundstelle im Amtsblatt einfügen sobald bekannt].

[17] [vollständigen Titel und Fundstelle im Amtsblatt einfügen sobald bekannt].

Änderungsantrag 9
Vorschlag für eine Richtlinie
Erwägung 15

Vorschlag der Kommission	*Geänderter Text*
(15) Die Beibehaltung eines zuverlässigen, resilienten und sicheren Domänennamensystems (DNS) ist ein Schlüsselfaktor für die Wahrung der Integrität des Internets und von entscheidender Bedeutung für dessen kontinuierlichen und stabilen Betrieb, von dem die digitale Wirtschaft und Gesellschaft abhängig ***ist***. Daher sollte die vorliegende Richtlinie für alle Anbieter von DNS-Diensten entlang der DNS-Auflösungskette ***gelten***, einschließlich Betreibern von Root-Namenservern, Namenservern der Domäne oberster Stufe (TLD-Namenservern), autoritativen Namenservern für Domänennamen und rekursiven Resolvern.	(15) Die Beibehaltung eines zuverlässigen, resilienten und sicheren Domänennamensystems (DNS) ist ein Schlüsselfaktor für die Wahrung der Integrität des Internets und von entscheidender Bedeutung für dessen kontinuierlichen und stabilen Betrieb, von dem die digitale Wirtschaft***, der Binnenmarkt*** und ***die*** Gesellschaft abhängig ***sind***. Daher sollte die vorliegende Richtlinie für alle Anbieter von DNS-Diensten entlang der DNS-Auflösungskette, einschließlich Betreibern von Root-Namenservern, Namenservern der Domäne oberster Stufe (TLD-Namenservern), autoritativen Namenservern für Domänennamen und rekursiven Resolvern ***und Anbietern von Datenschutz- oder Proxy-Registrierungsdiensten, Domänenmaklern oder Wiederverkäufern, und für alle anderen Dienste, die mit der Registrierung von Domänennamen zusammenhängen, gelten***.

Änderungsantrag 10
Vorschlag für eine Richtlinie
Erwägung 20

Vorschlag der Kommission	*Geänderter Text*
(20) Diese wachsenden gegenseitigen Abhängigkeiten sind das Ergebnis eines sich über immer mehr Grenzen hinweg erstreckenden und zunehmend interdependenten Dienstleistungsnetzes, das zentrale Infrastrukturen in der gesamten Union nutzt, und zwar in den Sektoren Energie, Verkehr, digitale Infrastruktur, Trinkwasser und Abwasser, Gesundheit, bestimmten Bereichen der öffentlichen Verwaltung sowie im Weltraumsektor, soweit es um die Erbringung bestimmter Dienste geht, die von Bodeninfrastrukturen abhängig sind, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden; damit sind Infrastrukturen ausgenommen, die sich im Eigentum der Union befinden oder von der Union oder in ihrem Namen im Rahmen ihrer Weltraumprogramme verwaltet oder betrieben werden. Wegen dieser gegenseitigen Abhängigkeiten kann jede Störung, auch wenn sie anfänglich auf eine Einrichtung oder einen Sektor beschränkt ist, zu breiteren Kaskadeneffekten führen, die weitreichende und lang anhaltende negative Auswirkungen auf die Erbringung von Dienstleistungen im gesamten Binnenmarkt haben können. Die COVID-19-Pandemie hat gezeigt, wie anfällig unsere zunehmend interdependenten Gesellschaften für Risiken mit geringer Eintrittswahrscheinlichkeit sind.	(20) Diese wachsenden gegenseitigen Abhängigkeiten sind das Ergebnis eines sich über immer mehr Grenzen hinweg erstreckenden und zunehmend interdependenten Dienstleistungsnetzes, das zentrale Infrastrukturen in der gesamten Union nutzt, und zwar in den Sektoren Energie, Verkehr, digitale Infrastruktur, Trinkwasser und Abwasser, Gesundheit, bestimmten Bereichen der öffentlichen Verwaltung sowie im Weltraumsektor, soweit es um die Erbringung bestimmter Dienste geht, die von Bodeninfrastrukturen abhängig sind, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden; damit sind Infrastrukturen ausgenommen, die sich im Eigentum der Union befinden oder von der Union oder in ihrem Namen im Rahmen ihrer Weltraumprogramme verwaltet oder betrieben werden. Wegen dieser gegenseitigen Abhängigkeiten kann jede Störung, auch wenn sie anfänglich auf eine Einrichtung oder einen Sektor beschränkt ist, zu breiteren Kaskadeneffekten führen, die weitreichende und lang anhaltende negative Auswirkungen auf die Erbringung von Dienstleistungen im gesamten Binnenmarkt haben können. Die COVID-19-Pandemie hat gezeigt, wie anfällig unsere zunehmend interdependenten Gesellschaften für Risiken mit geringer Eintrittswahrscheinlichkeit sind ***und dass der Binnenmarkt durch gemeinsame Strategien und Maßnahmen auf Unionsebene geschützt werden muss***.

Änderungsantrag 11
Vorschlag für eine Richtlinie
Erwägung 23

Vorschlag der Kommission	*Geänderter Text*
(23) Einrichtungen sollten den zuständigen Behörden oder den CSIRTs Sicherheitsvorfälle wirksam und effizient melden. Die zentralen Anlaufstellen sollten beauftragt werden, die Meldungen über Sicherheitsvorfälle an die zentralen Anlaufstellen anderer betroffener Mitgliedstaaten weiterzuleiten. Damit sichergestellt ist, dass es pro Mitgliedstaat nur eine einzige ***behördliche*** Anlaufstelle gibt, sollten die zentralen Anlaufstellen auch relevante Informationen über Vorfälle, die Einrichtungen des Finanzsektors betreffen, von den gemäß der Verordnung XXXX/XXXX zuständigen Behörden entgegennehmen, die sie gegebenenfalls gemäß der vorliegenden Richtlinie an die zuständigen nationalen Behörden oder CSIRTs weiterleiten können sollten.	(23) Einrichtungen sollten den zuständigen Behörden oder den CSIRTs Sicherheitsvorfälle ***auf standardisierte Weise sowie*** wirksam und effizient melden. Die zentralen Anlaufstellen sollten beauftragt werden, die Meldungen über Sicherheitsvorfälle an die zentralen Anlaufstellen anderer betroffener Mitgliedstaaten weiterzuleiten. Damit sichergestellt ist, dass es pro Mitgliedstaat nur eine einzige Anlaufstelle gibt, sollten die zentralen Anlaufstellen auch relevante Informationen über Vorfälle, die Einrichtungen des Finanzsektors betreffen, von den gemäß der Verordnung XXXX/XXXX zuständigen Behörden entgegennehmen, die sie gegebenenfalls gemäß der vorliegenden Richtlinie an die zuständigen nationalen Behörden oder CSIRTs weiterleiten können sollten.

Änderungsantrag 12
Vorschlag für eine Richtlinie
Erwägung 25

Vorschlag der Kommission	*Geänderter Text*
(25) In Bezug auf personenbezogene Daten sollten CSIRTs in der Lage sein, im Einklang mit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[19] im Namen und auf Ersuchen einer unter die vorliegende Richtlinie fallenden Einrichtung eine ***proaktive*** Überprüfung der für die Bereitstellung ihrer Dienste verwendeten Netz- und Informationssysteme auf Schwachstellen vorzunehmen. Die Mitgliedstaaten sollten für alle sektorbezogenen CSIRTs ein vergleichbares Niveau an technischen Kapazitäten anstreben. Die Mitgliedstaaten können die Agentur der Europäischen Union für Cybersicherheit (ENISA) um Unterstützung bei der Einsetzung	(25) In Bezug auf personenbezogene Daten sollten CSIRTs in der Lage sein, im Einklang mit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[19] im Namen und auf Ersuchen einer unter die vorliegende Richtlinie fallenden Einrichtung eine Überprüfung der für die Bereitstellung ihrer Dienste verwendeten Netz- und Informationssysteme auf Schwachstellen vorzunehmen***, um konkrete Bedrohungen in Bezug auf personenbezogene Daten zu erkennen, zu mindern und zu verhindern***. Die Mitgliedstaaten sollten für alle sektorbezogenen CSIRTs ein vergleichbares Niveau an technischen Kapazitäten anstreben. Die Mitgliedstaaten können die Agentur der Europäischen

nationaler CSIRTs ersuchen.	Union für Cybersicherheit (ENISA) um Unterstützung bei der Einsetzung nationaler CSIRTs ersuchen.
[19] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).	[19] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

Änderungsantrag 13
Vorschlag für eine Richtlinie
Erwägung 26 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(26a) Im Rahmen ihrer nationalen Cybersicherheitsstrategien sollten die Mitgliedstaaten Maßnahmen zur Förderung und Integration intelligenter Systeme bei der Prävention und Erkennung von Cybersicherheitsvorfällen und Cyberbedrohungen ergreifen. Die Mitgliedstaaten sollten im Einklang mit ihren nationalen Cybersicherheitsstrategien auf die Sensibilisierung für Cybersicherheit und einschlägige Kompetenzen ausgerichtete Maßnahmen einführen, um Verbraucher zu schützen. Bei der Annahme nationaler Cybersicherheitsstrategien sollten die Mitgliedstaaten für politische Rahmen für einen rechtmäßigen Zugang zu Informationen sorgen.

Änderungsantrag 14
Vorschlag für eine Richtlinie
Erwägung 27

Vorschlag der Kommission	*Geänderter Text*
(27) Im Einklang mit dem Anhang der Empfehlung (EU) 2017/***1548*** der Kommission für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen („Konzeptentwurf“)[20] sollte der Begriff ***„Sicherheitsvorfall großen Ausmaßes“*** einen Sicherheitsvorfall bezeichnen, der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat oder der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt. Je nach Ursache und Auswirkung können sich ***Sicherheitsvorfälle großen Ausmaßes*** verschärfen und zu echten Krisen entwickeln, die das reibungslose Funktionieren des Binnenmarkts verhindern. Angesichts der großen Tragweite und des, in den meisten Fällen, grenzübergreifenden Charakters solcher Sicherheitsvorfälle sollten die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union auf technischer, operativer und politischer Ebene zusammenarbeiten, um die Reaktion unionsweit angemessen zu koordinieren.	(27) Im Einklang mit dem Anhang der Empfehlung (EU) 2017/***1584*** der Kommission für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen („Konzeptentwurf“)[20] sollte der Begriff ***„großer Sicherheitsvorfall“*** einen Sicherheitsvorfall bezeichnen, der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat oder der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt***, und durch den somit der Binnenmarkt gefährdet wird***. Je nach Ursache und Auswirkung können sich ***große Sicherheitsvorfälle*** verschärfen und zu echten Krisen entwickeln, die das reibungslose Funktionieren des Binnenmarkts verhindern. Angesichts der großen Tragweite und des, in den meisten Fällen, grenzübergreifenden Charakters solcher Sicherheitsvorfälle sollten die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union auf technischer, operativer und politischer Ebene zusammenarbeiten, um die Reaktion unionsweit angemessen zu koordinieren.
[20] Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (ABl. L 239 vom 19.9.2017, S. 36).	[20] Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (ABl. L 239 vom 19.9.2017, S. 36).

Änderungsantrag 15
Vorschlag für eine Richtlinie
Erwägung 28

Vorschlag der Kommission	*Geänderter Text*
(28) Da durch die Ausnutzung von Schwachstellen in Netz- und Informationssystemen erhebliche	(28) Da durch die Ausnutzung von Schwachstellen in Netz- und Informationssystemen erhebliche

Störungen und Schäden verursacht werden können, ist die rasche Erkennung und Behebung dieser Schwachstellen ein wichtiger Faktor bei der Verringerung des Cybersicherheitsrisikos. Einrichtungen, die solche Systeme entwickeln, sollten daher geeignete Verfahren für die Behandlung von entdeckten Schwachstellen festlegen. Da Schwachstellen häufig von Dritten (meldenden Einrichtungen) entdeckt und gemeldet (offengelegt) werden, sollte der Hersteller oder Anbieter von IKT-Produkten oder -Diensten auch Verfahren einführen, damit er von Dritten Informationen über Schwachstellen entgegennehmen kann. Diesbezüglich enthalten die internationalen Normen ISO/IEC 30111 und ISO/IEC 29417 Leitlinien für die Behandlung von Schwachstellen bzw. die Offenlegung von Schwachstellen. In Bezug auf die Offenlegung von Schwachstellen ist die Koordinierung zwischen meldenden Einrichtungen und Herstellern oder Anbietern von IKT-Produkten oder -Diensten besonders wichtig. Die koordinierte Offenlegung von Schwachstellen erfolgt in einem strukturierten Prozess, in dem den Organisationen Schwachstellen in einer Weise gemeldet werden, die der Organisation die Diagnose und Behebung der Schwachstelle ermöglicht, bevor detaillierte Informationen über die Schwachstelle an Dritte oder die Öffentlichkeit weitergegeben werden. Die koordinierte Offenlegung von Schwachstellen sollte auch die Koordinierung zwischen der meldenden Einrichtung und der Organisation in Bezug auf den Zeitplan für die Behebung und Veröffentlichung von Schwachstellen umfassen.

Störungen und Schäden ***für Unternehmen und Verbraucher*** verursacht werden können, ist die rasche Erkennung und Behebung dieser Schwachstellen ein wichtiger Faktor bei der Verringerung des Cybersicherheitsrisikos. Einrichtungen, die solche Systeme entwickeln, sollten daher geeignete Verfahren für die Behandlung von entdeckten Schwachstellen festlegen. Da Schwachstellen häufig von Dritten (meldenden Einrichtungen) entdeckt und gemeldet (offengelegt) werden, sollte der Hersteller oder Anbieter von IKT-Produkten oder -Diensten auch Verfahren einführen, damit er von Dritten Informationen über Schwachstellen entgegennehmen kann. Diesbezüglich enthalten die internationalen Normen ISO/IEC 30111 und ISO/IEC 29417 Leitlinien für die Behandlung von Schwachstellen bzw. die Offenlegung von Schwachstellen. In Bezug auf die Offenlegung von Schwachstellen ist die Koordinierung zwischen meldenden Einrichtungen und Herstellern oder Anbietern von IKT-Produkten oder -Diensten besonders wichtig. Die koordinierte Offenlegung von Schwachstellen erfolgt in einem strukturierten Prozess, in dem den Organisationen Schwachstellen in einer Weise gemeldet werden, die der Organisation die Diagnose und Behebung der Schwachstelle ermöglicht, bevor detaillierte Informationen über die Schwachstelle an Dritte oder die Öffentlichkeit weitergegeben werden. Die koordinierte Offenlegung von Schwachstellen sollte auch die Koordinierung zwischen der meldenden Einrichtung und der Organisation in Bezug auf den Zeitplan für die Behebung und Veröffentlichung von Schwachstellen umfassen.

Änderungsantrag 16
Vorschlag für eine Richtlinie
Erwägung 28 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(28a) Die Kommission, die ENISA und die Mitgliedstaaten sollten die internationale Anpassung an Normen und vorliegende bewährte Verfahren der Branche im Bereich des Risikomanagements weiterhin fördern, beispielsweise in den Bereichen Bewertungen der Sicherheit der Lieferkette, Informationsaustausch und Offenlegung von Schwachstellen.

Änderungsantrag 17
Vorschlag für eine Richtlinie
Erwägung 30

Vorschlag der Kommission	*Geänderter Text*
(30) Der rechtzeitige Zugang zu korrekten Informationen über Schwachstellen, die IKT-Produkte und -Dienste beeinträchtigen, trägt zu einem besseren Cybersicherheitsrisikomanagement bei. In dieser Hinsicht sind öffentlich zugängliche Informationen über Schwachstellen nicht nur für Einrichtungen und deren Nutzer, sondern auch für die zuständigen nationalen Behörden und die CSIRTs ein wichtiges Instrument. Aus diesem Grund sollte die ENISA ***ein Schwachstellenregister*** einrichten, ***in dem*** wesentliche und wichtige Einrichtungen und deren Anbieter sowie***, auf freiwilliger Basis,*** Einrichtungen, die nicht in den Anwendungsbereich der vorliegenden Richtlinie fallen, Schwachstellen offenlegen und Informationen über die Schwachstellen bereitstellen, die es den Nutzern ermöglichen, geeignete Abhilfemaßnahmen zu ergreifen.	(30) Der rechtzeitige Zugang zu korrekten Informationen über Schwachstellen, die IKT-Produkte und -Dienste beeinträchtigen, trägt zu einem besseren Cybersicherheitsrisikomanagement bei. In dieser Hinsicht sind ***Quellen für*** öffentlich zugängliche Informationen über Schwachstellen nicht nur für Einrichtungen und deren Nutzer, sondern auch für die zuständigen nationalen Behörden und die CSIRTs ein wichtiges Instrument. Aus diesem Grund sollte die ENISA ***eine Schwachstellendatenbank*** einrichten, ***über die*** wesentliche und wichtige Einrichtungen und deren Anbieter sowie Einrichtungen, die nicht in den Anwendungsbereich der vorliegenden Richtlinie fallen, ***auf freiwilliger Basis*** Schwachstellen offenlegen und Informationen über die Schwachstellen bereitstellen ***können***, die es den Nutzern ermöglichen, geeignete Abhilfemaßnahmen zu ergreifen.

Änderungsantrag 18
Vorschlag für eine Richtlinie
Erwägung 31

Vorschlag der Kommission	*Geänderter Text*
(31) Es gibt zwar bereits ähnliche Register oder Datenbanken für Schwachstellen, aber diese werden von Einrichtungen betrieben und gepflegt, die nicht in der Union niedergelassen sind. ***Ein*** von der ENISA ***gepflegtes europäisches Schwachstellenregister*** würde für mehr Transparenz in Bezug auf den Prozess der Veröffentlichung vor der offiziellen Offenlegung der Schwachstelle sorgen und die Resilienz im Falle von Störungen oder Unterbrechungen bei der Erbringung ähnlicher Dienste verbessern. Um Doppelarbeit zu vermeiden und im Interesse der größtmöglichen Komplementarität***,*** sollte die ENISA die Möglichkeit prüfen, Vereinbarungen über eine strukturierte Zusammenarbeit mit ***ähnlichen*** Registern in Drittländern zu schließen.	(31) Es gibt zwar bereits ähnliche Register oder Datenbanken für Schwachstellen, aber diese werden von Einrichtungen betrieben und gepflegt, die nicht in der Union niedergelassen sind. ***Eine*** von der ENISA ***gepflegte europäische Schwachstellendatenbank*** würde für mehr Transparenz in Bezug auf den Prozess der Veröffentlichung vor der offiziellen Offenlegung der Schwachstelle sorgen und die Resilienz im Falle von Störungen oder Unterbrechungen bei der Erbringung ähnlicher Dienste verbessern. Um Doppelarbeit zu vermeiden und im Interesse der größtmöglichen Komplementarität sollte die ENISA die Möglichkeit prüfen, Vereinbarungen über eine strukturierte Zusammenarbeit mit ***Datenbanken oder*** Registern ***für Schwachstellen*** in Drittländern zu schließen ***und Berichte an entsprechende Register zu übermitteln, sofern durch derartige Maßnahmen nicht der Schutz der Vertraulichkeit und von Betriebs- und Geschäftsgeheimnissen untergraben wird***.

Änderungsantrag 19
Vorschlag für eine Richtlinie
Erwägung 32

Vorschlag der Kommission	*Geänderter Text*
(32) Die Kooperationsgruppe sollte alle zwei Jahre ein Arbeitsprogramm aufstellen, in dem die Maßnahmen aufgeführt sind, die die Gruppe zur Umsetzung ihrer Ziele und Aufgaben zu ergreifen hat. Der Zeitrahmen des ersten Programms, das gemäß der vorliegenden Richtlinie angenommen wird, sollte an den	(32) Die Kooperationsgruppe sollte ***politische Prioritäten und wesentliche Herausforderungen in Bezug auf die Cybersicherheit erörtern und*** alle zwei Jahre ein Arbeitsprogramm aufstellen, in dem die Maßnahmen aufgeführt sind, die die Gruppe zur Umsetzung ihrer Ziele und Aufgaben zu ergreifen hat. Der Zeitrahmen

Zeitrahmen des letzten gemäß der Richtlinie (EU) 2016/1148 angenommenen Programms angepasst werden, um etwaige Unterbrechungen der Arbeit der Gruppe zu vermeiden.

des ersten Programms, das gemäß der vorliegenden Richtlinie angenommen wird, sollte an den Zeitrahmen des letzten gemäß der Richtlinie (EU) 2016/1148 angenommenen Programms angepasst werden, um etwaige Unterbrechungen der Arbeit der Gruppe zu vermeiden.

Änderungsantrag 20
Vorschlag für eine Richtlinie
Erwägung 32 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(32a) Die Kooperationsgruppe sollte sich aus Vertretern der Mitgliedstaaten, der Kommission und der ENISA zusammensetzen.

Änderungsantrag 21
Vorschlag für eine Richtlinie
Erwägung 34

Vorschlag der Kommission	*Geänderter Text*
(34) Die Kooperationsgruppe sollte ein flexibles Forum bleiben und in der Lage sein, unter Berücksichtigung der verfügbaren Ressourcen auf sich ändernde und neue politische Prioritäten und Herausforderungen zu reagieren. Sie sollte regelmäßige gemeinsame Sitzungen mit einschlägigen privaten Interessenträgern aus der gesamten Union organisieren, um die Tätigkeiten der Gruppe zu erörtern und Beiträge zu neuen politischen Herausforderungen einzuholen. Um die Zusammenarbeit auf Unionsebene zu verbessern, sollte die Gruppe in Erwägung ziehen, mit Cybersicherheitspolitik befasste Einrichtungen und Agenturen der Union, etwa das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3), die Agentur der Europäischen Union für Flugsicherheit (EASA) und die Agentur der Europäischen Union für das	(34) Die Kooperationsgruppe sollte ein flexibles Forum bleiben und in der Lage sein, unter Berücksichtigung der verfügbaren Ressourcen auf sich ändernde und neue politische Prioritäten und Herausforderungen zu reagieren. Sie sollte regelmäßige gemeinsame Sitzungen mit einschlägigen privaten Interessenträgern aus der gesamten Union organisieren, um die Tätigkeiten der Gruppe zu erörtern und Beiträge zu neuen politischen Herausforderungen einzuholen. Um die Zusammenarbeit auf Unionsebene zu verbessern, sollte die Gruppe in Erwägung ziehen, mit Cybersicherheitspolitik befasste Einrichtungen und Agenturen der Union, etwa das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3), die Agentur der Europäischen Union für Flugsicherheit (EASA) und die Agentur der Europäischen Union für das

Weltraumprogramm (EUSPA), zur Teilnahme an ihrer Arbeit einzuladen.	Weltraumprogramm (EUSPA), ***sowie weitere relevante Einrichtungen und Agenturen der Union*** zur Teilnahme an ihrer Arbeit einzuladen.

Änderungsantrag 22
Vorschlag für eine Richtlinie
Erwägung 35

Vorschlag der Kommission	*Geänderter Text*
(35) Die zuständigen Behörden und CSIRTs sollten befugt sein, an Austauschprogrammen für Bedienstete aus anderen Mitgliedstaaten teilzunehmen, um die Zusammenarbeit zu verbessern. Die zuständigen Behörden sollten Maßnahmen ergreifen, damit die Bediensteten aus anderen Mitgliedstaaten bei den Tätigkeiten der aufnehmenden zuständigen Behörde konstruktiv mitwirken können.	(35) Die zuständigen Behörden und CSIRTs sollten befugt sein, an Austauschprogrammen ***und gemeinsamen Schulungsprogrammen*** für Bedienstete aus anderen Mitgliedstaaten teilzunehmen, um die Zusammenarbeit zu verbessern ***und das Vertrauen zwischen den Mitgliedstaaten zu stärken***. Die zuständigen Behörden sollten Maßnahmen ergreifen, damit die Bediensteten aus anderen Mitgliedstaaten bei den Tätigkeiten der aufnehmenden zuständigen Behörde ***oder des aufnehmenden CSIRT*** konstruktiv mitwirken können.

Änderungsantrag 23
Vorschlag für eine Richtlinie
Erwägung 39

Vorschlag der Kommission	*Geänderter Text*
(39) Für die Zwecke der vorliegenden Richtlinie sollte sich der Begriff „Beinahe-Vorfälle“ auf ein Ereignis beziehen, das das Potenzial gehabt hätte, Schäden zu verursachen, dessen vollständiger Eintritt jedoch verhindert wurde.	***entfällt***

Änderungsantrag 24
Vorschlag für eine Richtlinie
Erwägung 45 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(45a) Darüber hinaus sollten Einrichtungen auch für eine angemessene Aus- und Weiterbildung ihres Personals im Bereich Cybersicherheit auf allen Ebenen der Organisation sorgen.

Änderungsantrag 25
Vorschlag für eine Richtlinie
Erwägung 46

Vorschlag der Kommission	*Geänderter Text*
(46) Um die Hauptrisiken für die Lieferkette weiter anzugehen und den Einrichtungen in den unter diese Richtlinie fallenden Sektoren dabei zu helfen, Cybersicherheitsrisiken in Bezug auf die Lieferkette und die Lieferanten angemessen zu beherrschen, sollte die Kooperationsgruppe, an der die einschlägigen nationalen Behörden beteiligt sind, in Zusammenarbeit mit der Kommission und der ENISA koordinierte sektorenbezogene Lieferketten-Risikobewertungen – wie im Fall der 5G-Netze gemäß der ***einschlägigen*** Empfehlung (EU) 2019/***534***[21] – durchführen, um ***für jeden*** Sektor die kritischen IKT-Dienste, -Systeme oder -Produkte sowie relevante Bedrohungen und Schwachstellen zu ermitteln.	(46) Um die Hauptrisiken für die Lieferkette weiter anzugehen und den Einrichtungen in den unter diese Richtlinie fallenden Sektoren dabei zu helfen, Cybersicherheitsrisiken in Bezug auf die Lieferkette und die Lieferanten angemessen zu beherrschen, sollte die Kooperationsgruppe, an der die einschlägigen nationalen Behörden beteiligt sind, in Zusammenarbeit mit der Kommission und der ENISA koordinierte sektorenbezogene Lieferketten-Risikobewertungen – wie im Fall der 5G-Netze gemäß der Empfehlung (EU) 2019/***534 zur Cybersicherheit der 5G-Netze***[21] – durchführen, um ***in jedem*** Sektor die kritischen IKT-Dienste, -Systeme oder -Produkte sowie relevante Bedrohungen und Schwachstellen zu ermitteln.
[21] Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019 Cybersicherheit der 5G-Netze (ABl. L 88 vom 29.3.2019, S. 42).	[21] Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019 Cybersicherheit der 5G-Netze (ABl. L 88 vom 29.3.2019, S. 42).

Änderungsantrag 26
Vorschlag für eine Richtlinie
Erwägung 47

Vorschlag der Kommission	*Geänderter Text*
(47) Bei den Lieferketten-Risikobewertungen unter Berücksichtigung der Besonderheiten des jeweiligen Sektors sollte sowohl technischen wie auch gegebenenfalls nichttechnischen Faktoren Rechnung getragen werden, einschließlich derer, die in der Empfehlung (EU) 2019/534, in der EU-weit koordinierten Risikobewertung zur Cybersicherheit in 5G-Netzen sowie in dem von der Kooperationsgruppe vereinbarten EU-Instrumentarium für die 5G-Cybersicherheit definiert sind. Bei der Ermittlung der Lieferketten, die einer koordinierten Risikobewertung unterzogen werden sollten, sollten folgende Kriterien berücksichtigt werden: i) der Umfang, in dem wesentliche und wichtige Einrichtungen bestimmte kritische IKT-Dienste, -Systeme oder -Produkte nutzen und auf sie angewiesen sind; ii) die Bedeutung bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte für die Ausführung kritischer oder sensibler Funktionen, einschließlich der Verarbeitung personenbezogener Daten; iii) die Verfügbarkeit alternativer IKT-Dienste, -Systeme oder -Produkte; iv) die Resilienz der gesamten Lieferkette von IKT-Diensten, -Systemen oder -Produkten gegen destabilisierende Ereignisse und v) die potenzielle künftige Bedeutung neuer IKT-Dienste, -Systeme oder -Produkte für die Tätigkeiten der Einrichtungen.	(47) Bei den Lieferketten-Risikobewertungen unter Berücksichtigung der Besonderheiten des jeweiligen Sektors ***und seiner Kritikalität*** sollte sowohl technischen wie auch gegebenenfalls nichttechnischen Faktoren Rechnung getragen werden, einschließlich derer, die in der Empfehlung (EU) 2019/534, in der EU-weit koordinierten Risikobewertung zur Cybersicherheit in 5G-Netzen sowie in dem von der Kooperationsgruppe vereinbarten EU-Instrumentarium für die 5G-Cybersicherheit definiert sind. Bei der Ermittlung der Lieferketten, die einer koordinierten Risikobewertung unterzogen werden sollten, sollten folgende Kriterien berücksichtigt werden: i) der Umfang, in dem wesentliche und wichtige Einrichtungen bestimmte kritische IKT-Dienste, -Systeme oder -Produkte nutzen und auf sie angewiesen sind; ii) die Bedeutung bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte für die Ausführung kritischer oder sensibler Funktionen, einschließlich der Verarbeitung personenbezogener Daten; iii) die Verfügbarkeit alternativer IKT-Dienste, -Systeme oder -Produkte; iv) die Resilienz der gesamten Lieferkette von IKT-Diensten, -Systemen oder -Produkten gegen destabilisierende Ereignisse und v) die potenzielle künftige Bedeutung neuer IKT-Dienste, -Systeme oder -Produkte für die Tätigkeiten der Einrichtungen.

Änderungsantrag 27
Vorschlag für eine Richtlinie
Erwägung 51

Vorschlag der Kommission	*Geänderter Text*
(51) Das Funktionieren des Internets ist für den Binnenmarkt wichtiger denn je. Die Dienstleistungen praktisch aller wesentlichen und wichtigen Einrichtungen	(51) Das Funktionieren des Internets ist für den Binnenmarkt wichtiger denn je. Die Dienstleistungen praktisch aller wesentlichen und wichtigen Einrichtungen

hängen ihrerseits von Diensten ab, die über das Internet erbracht werden. Für die reibungslose Bereitstellung von Diensten wesentlicher und wichtiger Einrichtungen ist es wichtig, dass für öffentliche elektronische Kommunikationsnetze, z. B. Internet-Backbone- oder Seekabel, geeignete Cybersicherheitsmaßnahmen bestehen und diesbezügliche Sicherheitsvorfälle gemeldet werden.

hängen ihrerseits von Diensten ab, die über das Internet erbracht werden***, und die Verbraucher sind in wesentlichen Bereichen ihres täglichen Lebens davon abhängig***. Für die reibungslose Bereitstellung von Diensten wesentlicher und wichtiger Einrichtungen ist es wichtig, dass für öffentliche elektronische Kommunikationsnetze, z. B. Internet-Backbone- oder Seekabel, geeignete Cybersicherheitsmaßnahmen bestehen und diesbezügliche Sicherheitsvorfälle gemeldet werden.

Änderungsantrag 28
Vorschlag für eine Richtlinie
Erwägung 52

Vorschlag der Kommission	*Geänderter Text*
(52) ***Gegebenenfalls*** sollten ***die Einrichtungen*** die Empfänger ihrer Dienste über besondere und erhebliche Bedrohungen sowie über Maßnahmen informieren, die sie ergreifen können, um das sich daraus ergebende Risiko für sich selbst zu mindern***. Die Verpflichtung zur Information*** der ***Empfänger über solche Bedrohungen sollte*** die Einrichtungen nicht von der Pflicht ***befreien***, auf eigene Kosten angemessene Sofortmaßnahmen zu ergreifen, um jedwede Cyberbedrohung zu verhüten oder zu beseitigen und das normale Sicherheitsniveau des Dienstes wiederherzustellen. Die Bereitstellung solcher Informationen über Sicherheitsbedrohungen ***sollte*** für die Empfänger kostenlos sein.	(52) ***Die Einrichtungen*** sollten ***bestrebt sein,*** die Empfänger ihrer Dienste über besondere und erhebliche Bedrohungen sowie über Maßnahmen ***zu*** informieren, die sie ergreifen können, um das sich daraus ergebende Risiko für sich selbst zu mindern***, insbesondere, wenn durch solche Maßnahmen*** der ***Verbraucherschutz verbessert werden kann. Dadurch sollten*** die Einrichtungen nicht von der Pflicht ***befreit werden***, auf eigene Kosten angemessene Sofortmaßnahmen zu ergreifen, um jedwede Cyberbedrohung zu verhüten oder zu beseitigen und das normale Sicherheitsniveau des Dienstes wiederherzustellen. Die Bereitstellung solcher Informationen über Sicherheitsbedrohungen für die Empfänger ***sollte*** kostenlos sein***, und die Informationen sollten in leicht verständlicher Sprache bereitgestellt werden***.

Änderungsantrag 29
Vorschlag für eine Richtlinie
Erwägung 53

Vorschlag der Kommission	*Geänderter Text*
(53) Insbesondere sollten die Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste die Empfänger der Dienste über besondere und erhebliche Cyberbedrohungen sowie über Maßnahmen zum Schutz von Kommunikationsinhalten, die sie treffen können, informieren, z. B. den Einsatz spezieller Software oder von Verschlüsselungsverfahren.	(53) Insbesondere sollten die Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste die Empfänger der Dienste über besondere und erhebliche Cyberbedrohungen sowie über ***zusätzliche*** Maßnahmen zum Schutz ***der Sicherheit ihrer Geräte und*** von Kommunikationsinhalten, die sie treffen können, informieren, z. B. den Einsatz spezieller Software oder von Verschlüsselungsverfahren.

Änderungsantrag 30
Vorschlag für eine Richtlinie
Erwägung 54

Vorschlag der Kommission	*Geänderter Text*
(54) Zur Aufrechterhaltung der Sicherheit elektronischer Kommunikationsnetze und -dienste sollte die Verschlüsselung, insbesondere von Ende zu Ende, gefördert werden; erforderlichenfalls sollte sie für die Anbieter solcher Dienste und Netze im Einklang mit den Grundsätzen der Sicherheit und des Schutzes der Privatsphäre mittels datenschutzfreundlicher Voreinstellungen und Technikgestaltung für die Zwecke ***des Artikels 18*** vorgeschrieben werden. Die Nutzung der End-zu-End-Verschlüsselung ***sollte mit den Befugnissen*** der Mitgliedstaaten, den Schutz ihrer wesentlichen Sicherheitsinteressen und der öffentlichen Sicherheit zu gewährleisten und die Ermittlung, Aufdeckung und Verfolgung von Straftaten im Einklang mit dem Unionsrecht zu ermöglichen***, in Einklang gebracht werden***. Lösungen für	(54) Zur Aufrechterhaltung der Sicherheit elektronischer Kommunikationsnetze und -dienste sollte die Verschlüsselung, insbesondere von Ende zu Ende, gefördert werden; erforderlichenfalls sollte sie für die Anbieter solcher Dienste und Netze im Einklang mit den Grundsätzen der Sicherheit und des Schutzes der Privatsphäre mittels datenschutzfreundlicher Voreinstellungen und Technikgestaltung für die Zwecke ***von Risikomanagementmaßnahmen im Bereich der Cybersicherheit*** vorgeschrieben werden. Die Nutzung der End-zu-End-Verschlüsselung ***berührt nicht die Befugnisse, Maßnahmen und Verfahren*** der Mitgliedstaaten ***in Bezug darauf***, den Schutz ihrer wesentlichen Sicherheitsinteressen und der öffentlichen Sicherheit zu gewährleisten und die Ermittlung, Aufdeckung und Verfolgung

den rechtmäßigen Zugang zu Informationen in End-zu-End-verschlüsselter Kommunikation sollten die Wirksamkeit der Verschlüsselung beim Schutz der Privatsphäre und der Sicherheit der Kommunikation aufrechterhalten und zugleich eine wirksame Reaktion auf Straftaten gewährleisten.	von Straftaten im Einklang mit dem Unionsrecht zu ermöglichen. Lösungen für den rechtmäßigen Zugang zu Informationen in End-zu-End-verschlüsselter Kommunikation sollten die Wirksamkeit der Verschlüsselung beim Schutz der Privatsphäre und der Sicherheit der Kommunikation aufrechterhalten und zugleich eine wirksame Reaktion auf Straftaten gewährleisten. ***Bei jeglichen ergriffenen Maßnahmen sind die Grundsätze der Verhältnismäßigkeit und der Subsidiarität strikt einzuhalten.***

Änderungsantrag 31
Vorschlag für eine Richtlinie
Erwägung 55

Vorschlag der Kommission	*Geänderter Text*
(55) Mit dieser Richtlinie wird ein ***zweistufiger*** Ansatz für die Meldung von Sicherheitsvorfällen festgelegt, um die richtige Balance herzustellen zwischen einer zeitnahen Meldung einerseits, die einer potenziellen Ausbreitung von Sicherheitsvorfällen entgegenwirkt und den Einrichtungen die Möglichkeit gibt, Unterstützung zu erhalten, und einer detaillierten Meldung andererseits, bei der aus individuellen Sicherheitsvorfällen wichtige Lehren gezogen werden und einzelne Unternehmen und ganze Sektoren ihre Resilienz gegenüber Cyberbedrohungen im Laufe der Zeit verbessern können. Erhalten Einrichtungen Kenntnis von einem Sicherheitsvorfall, sollten sie innerhalb von ***24*** Stunden eine erste Meldung übermitteln und spätestens einen Monat ***danach*** einen Abschlussbericht vorlegen müssen. Die Erstmeldung sollte nur die Informationen enthalten, die unbedingt erforderlich sind, um die zuständigen Behörden über den Sicherheitsvorfall zu unterrichten und es der Einrichtung zu ermöglichen, bei Bedarf Hilfe in Anspruch zu nehmen. Gegebenenfalls sollte aus dieser Meldung	(55) Mit dieser Richtlinie wird ein ***mehrstufiger*** Ansatz für die Meldung von Sicherheitsvorfällen festgelegt, um die richtige Balance herzustellen zwischen einer zeitnahen Meldung einerseits, die einer potenziellen Ausbreitung von Sicherheitsvorfällen entgegenwirkt und den Einrichtungen die Möglichkeit gibt, Unterstützung zu erhalten, und einer detaillierten Meldung andererseits, bei der aus individuellen Sicherheitsvorfällen wichtige Lehren gezogen werden und einzelne Unternehmen und ganze Sektoren ihre Resilienz gegenüber Cyberbedrohungen im Laufe der Zeit verbessern können. Erhalten Einrichtungen Kenntnis von einem Sicherheitsvorfall ***oder einem Beinahe-Vorfall***, sollten sie innerhalb von ***72*** Stunden eine erste Meldung übermitteln***, spätestens drei Monate nach der Übermittlung der ersten Meldung einen umfassenden Bericht vorlegen*** und spätestens einen Monat ***nach der Eindämmung des Vorfalls*** einen Abschlussbericht vorlegen müssen. Die Erstmeldung sollte nur die Informationen enthalten, die unbedingt erforderlich sind, um die zuständigen Behörden über den

hervorgehen, ob der Sicherheitsvorfall vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist. Die Mitgliedstaaten sollten sicherstellen, dass durch die Pflicht zur Übermittlung dieser Erstmeldung die Ressourcen der meldenden Einrichtung für Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen, die Vorrang haben sollten, nicht beeinträchtigt werden. Zur weiteren Verhinderung, dass die Meldepflichten für Sicherheitsvorfälle entweder zulasten der Ressourcen gehen, auf solche Vorfälle zu reagieren, oder entsprechende Anstrengungen der Einrichtungen anderweitig beeinträchtigt werden, sollten die Mitgliedstaaten auch vorsehen, dass die betreffende Einrichtung in hinreichend begründeten Fällen und im Einvernehmen mit den zuständigen Behörden oder dem CSIRT von ***der Frist von 24 Stunden für die Erstmeldung bzw. einem Monat für den Abschlussbericht*** abweichen kann.

Sicherheitsvorfall zu unterrichten und es der Einrichtung zu ermöglichen, bei Bedarf Hilfe in Anspruch zu nehmen. Gegebenenfalls sollte aus dieser Meldung hervorgehen, ob der Sicherheitsvorfall vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist. Die Mitgliedstaaten sollten sicherstellen, dass durch die Pflicht zur Übermittlung dieser Erstmeldung die Ressourcen der meldenden Einrichtung für Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen, die Vorrang haben sollten, nicht beeinträchtigt werden. ***Vor der Übermittlung der Erstmeldung sollte in den ersten 24 Stunden eine Frühwarnung übermittelt werden, wobei keine Verpflichtung zur Offenlegung zusätzlicher Informationen besteht. Diese Frühwarnung sollte so bald wie möglich übermittelt werden, damit Einrichtungen rasch um die Unterstützung der zuständigen Behörden oder von CSIRTs ersuchen können und die zuständigen Behörden oder CSIRTs die potenzielle Ausbreitung des gemeldeten Vorfalls begrenzen können, und sollte als Instrument zur Lageerfassung für CSIRTs dienen.*** Zur weiteren Verhinderung ***dessen***, dass die Meldepflichten für Sicherheitsvorfälle entweder zulasten der Ressourcen ***dafür*** gehen, auf solche Vorfälle zu reagieren, oder entsprechende Anstrengungen der Einrichtungen anderweitig beeinträchtigt werden, sollten die Mitgliedstaaten auch vorsehen, dass die betreffende Einrichtung in hinreichend begründeten Fällen und im Einvernehmen mit den zuständigen Behörden oder dem CSIRT von ***den vorgesehenen Fristen*** abweichen kann.

Änderungsantrag 32
Vorschlag für eine Richtlinie
Erwägung 56

Vorschlag der Kommission	*Geänderter Text*
(56) Wesentliche und wichtige Einrichtungen sind häufig in einer Situation, in der ein bestimmter Sicherheitsvorfall aufgrund seiner Merkmale und sich aus verschiedenen Rechtsinstrumenten ergebender Meldepflichten verschiedenen Behörden gemeldet werden muss. Solche Fälle führen zu zusätzlichen Belastungen und unter Umständen auch zu Unsicherheiten hinsichtlich des Formats solcher Meldungen und der für sie geltenden Verfahren. Vor diesem Hintergrund und zur Vereinfachung der Meldung von Sicherheitsvorfällen sollten die Mitgliedstaaten eine zentrale Anlaufstelle für alle Meldungen einrichten, die aufgrund dieser Richtlinie sowie anderer EU-Rechtsvorschriften wie der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG vorgeschrieben sind. Die ENISA sollte in Zusammenarbeit mit der Kooperationsgruppe mittels Leitlinien einheitliche Meldemuster erstellen, die die im Unionsrecht geforderten Informationen vereinfachen und straffen und den Aufwand für die Unternehmen verringern würden.	(56) Wesentliche und wichtige Einrichtungen sind häufig in einer Situation, in der ein bestimmter Sicherheitsvorfall aufgrund seiner Merkmale und sich aus verschiedenen Rechtsinstrumenten ergebender Meldepflichten verschiedenen Behörden gemeldet werden muss. Solche Fälle führen zu zusätzlichen Belastungen und unter Umständen auch zu Unsicherheiten hinsichtlich des Formats solcher Meldungen und der für sie geltenden Verfahren. Vor diesem Hintergrund und zur Vereinfachung der Meldung von Sicherheitsvorfällen ***und zur Wahrung des Grundsatzes der Einmaligkeit*** sollten die Mitgliedstaaten eine zentrale Anlaufstelle für alle Meldungen einrichten, die aufgrund dieser Richtlinie sowie anderer EU-Rechtsvorschriften wie der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG vorgeschrieben sind. Die ENISA sollte in Zusammenarbeit mit der Kooperationsgruppe mittels Leitlinien einheitliche Meldemuster erstellen, die die im Unionsrecht geforderten Informationen vereinfachen und straffen und den Aufwand für die Unternehmen verringern würden.

Änderungsantrag 33
Vorschlag für eine Richtlinie
Erwägung 59

Vorschlag der Kommission	*Geänderter Text*
(59) Die Pflege genauer und vollständiger Datenbanken mit Domänennamen und Registrierungsdaten (sogenannte „WHOIS-Daten“) und ein rechtmäßiger Zugang zu diesen Daten sind entscheidend, um die Sicherheit, Stabilität und Resilienz des DNS zu gewährleisten, was wiederum zu einem hohen gemeinsamen Cybersicherheitsniveau in	(59) Die Pflege genauer***, überprüfter*** und vollständiger Datenbanken mit Domänennamen und Registrierungsdaten (sogenannte „WHOIS-Daten“) und ein rechtmäßiger Zugang zu diesen Daten sind entscheidend, um die Sicherheit, Stabilität und Resilienz des DNS zu gewährleisten, was wiederum zu einem hohen gemeinsamen Cybersicherheitsniveau in

der Union beiträgt. Werden auch personenbezogene Daten verarbeitet, so muss diese Verarbeitung mit dem EU-Datenschutzrecht im Einklang stehen.

der Union beiträgt. Werden auch personenbezogene Daten verarbeitet, so muss diese Verarbeitung mit dem EU-Datenschutzrecht im Einklang stehen.

Änderungsantrag 34
Vorschlag für eine Richtlinie
Erwägung 61

Vorschlag der Kommission	*Geänderter Text*
(61) Zur Gewährleistung der Verfügbarkeit genauer und vollständiger Domänennamen-Registrierungsdaten sollten die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste ***für*** die ***TLD erbringen (sogenannte Registrierstellen***), die Integrität und Verfügbarkeit von Domänennamen-Registrierungsdaten erfassen und garantieren. Insbesondere sollten die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, Grundsätze und Verfahren festlegen, um im Einklang mit den EU-Datenschutzvorschriften genaue und vollständige Registrierungsdaten zu erfassen und zu pflegen sowie unrichtige Registrierungsdaten zu verhindern bzw. zu berichtigen.	(61) Zur Gewährleistung der Verfügbarkeit genauer und vollständiger Domänennamen-Registrierungsdaten sollten die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste ***(einschließlich Diensten von Domänennamen-Registern und -Registrierstellen, Anbietern von Datenschutz- oder Proxy-Registrierungsdiensten, Domänenmaklern oder Wiederverkäufern sowie einschließlich jeglicher anderer Dienste,*** die ***mit der Registrierung von Domänennamen zusammenhängen***) ***erbringen***, die Integrität und Verfügbarkeit von Domänennamen-Registrierungsdaten erfassen und garantieren. Insbesondere sollten die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, Grundsätze und Verfahren festlegen, um im Einklang mit den EU-Datenschutzvorschriften genaue und vollständige Registrierungsdaten zu erfassen und zu pflegen sowie unrichtige Registrierungsdaten zu verhindern bzw. zu berichtigen.

Änderungsantrag 35
Vorschlag für eine Richtlinie
Erwägung 68

Vorschlag der Kommission	*Geänderter Text*
(68) Die Einrichtungen sollten ermutigt	(68) Die Einrichtungen sollten ermutigt

werden, ihre individuellen Kenntnisse und praktischen Erfahrungen auf strategischer, taktischer und operativer Ebene gemeinsam zu nutzen, damit sich ihre Fähigkeit verbessert, Cyberbedrohungen angemessen zu bewerten, zu überwachen**,** abzuwehren und auf sie zu reagieren. Daher muss dafür gesorgt werden, dass auf Unionsebene Mechanismen für Vereinbarungen über den freiwilligen Informationsaustausch entstehen können. Zu diesem Zweck sollten die Mitgliedstaaten auch einschlägige Einrichtungen, die nicht unter diese Richtlinie fallen, aktiv unterstützen und dazu anhalten, sich an solchen Mechanismen zum Informationsaustausch zu beteiligen. Diese Mechanismen sollten unter uneingeschränkter Einhaltung der Wettbewerbsvorschriften und des Datenschutzrechts der Union eingerichtet werden.

und von den Mitgliedstaaten dabei unterstützt werden, ihre individuellen Kenntnisse und praktischen Erfahrungen auf strategischer, taktischer und operativer Ebene gemeinsam zu nutzen, damit sich ihre Fähigkeit verbessert, Cyberbedrohungen angemessen zu bewerten, zu überwachen ***und*** abzuwehren und auf sie zu reagieren. Daher muss dafür gesorgt werden, dass auf Unionsebene Mechanismen für Vereinbarungen über den freiwilligen Informationsaustausch entstehen können. Zu diesem Zweck sollten die Mitgliedstaaten auch einschlägige Einrichtungen, die nicht unter diese Richtlinie fallen, aktiv unterstützen und dazu anhalten, sich an solchen Mechanismen zum Informationsaustausch zu beteiligen. Diese Mechanismen sollten unter uneingeschränkter Einhaltung der Wettbewerbsvorschriften und des Datenschutzrechts der Union eingerichtet werden.

Änderungsantrag 36
Vorschlag für eine Richtlinie
Erwägung 69

Vorschlag der Kommission	*Geänderter Text*
(69) Die Verarbeitung personenbezogener Daten durch Einrichtungen, Behörden, CERTs, CSIRTs sowie Anbieter von Sicherheitstechnologien und -diensten ***sollte im Sinne der Verordnung (EU) 2016/679 ein berechtigtes Interesse des jeweiligen Verantwortlichen darstellen***, ***wie dies*** für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist. Dies sollte auch Folgendes einschließen: Maßnahmen im Hinblick auf die Verhütung, Erkennung, Analyse und Bewältigung von Sicherheitsvorfällen, Maßnahmen zur Sensibilisierung für spezifische Cyberbedrohungen, Informationsaustausch im Zusammenhang	(69) Die Verarbeitung personenbezogener Daten durch Einrichtungen, Behörden, CERTs, CSIRTs sowie Anbieter von Sicherheitstechnologien und -diensten***, die auf das begrenzt werden sollte***, ***was*** für die Gewährleistung der Netz- und Informationssicherheit ***und die Sicherstellung des Verbraucherschutzes*** unbedingt notwendig und verhältnismäßig ist***, sollte im Sinne der Verordnung (EU) 2016/679 ein berechtigtes Interesse des jeweiligen Verantwortlichen darstellen***. Dies sollte auch Folgendes einschließen: Maßnahmen im Hinblick auf die Verhütung, Erkennung, Analyse und Bewältigung von Sicherheitsvorfällen, Maßnahmen zur Sensibilisierung für

mit der Behebung von Schwachstellen und ihrer koordinierten Offenlegung, freiwilliger Austausch von Informationen über solche Sicherheitsvorfälle sowie über Cyberbedrohungen und Schwachstellen, Gefährdungsindikatoren, Taktiken, Vorgehensweisen und Verfahren, Cybersicherheitswarnungen und Konfigurationstools. Diese Maßnahmen können die Verarbeitung folgender Arten personenbezogener Daten erfordern: IP-Adressen, Uniform Resource Locators (URL-Adressen), Domänennamen und E-Mail-Adressen.

spezifische Cyberbedrohungen, Informationsaustausch im Zusammenhang mit der Behebung von Schwachstellen und ihrer koordinierten Offenlegung, freiwilliger Austausch von Informationen über solche Sicherheitsvorfälle sowie über Cyberbedrohungen und Schwachstellen, Gefährdungsindikatoren, Taktiken, Vorgehensweisen und Verfahren, Cybersicherheitswarnungen und Konfigurationstools. Diese Maßnahmen können die Verarbeitung folgender Arten personenbezogener Daten erfordern: IP-Adressen, Uniform Resource Locators (URL-Adressen), Domänennamen und E-Mail-Adressen.

Änderungsantrag 37
Vorschlag für eine Richtlinie
Erwägung 70

Vorschlag der Kommission

(70) Zur Stärkung der Aufsichtsbefugnisse und der Maßnahmen, die zu einer wirksamen Befolgung der Vorschriften beitragen, sollte diese Richtlinie einen Mindestumfang an Aufsichtsmaßnahmen und -mitteln vorsehen, mit welchen die zuständigen Behörden wesentliche und wichtige Einrichtungen beaufsichtigen können. Darüber hinaus sollte in dieser Richtlinie eine Abgrenzung zwischen den Aufsichtssystemen für wesentliche und für wichtige Einrichtungen vorgenommen werden, um die Verpflichtungen sowohl für die Einrichtungen als auch für die zuständigen Behörden ausgewogen zu gestalten. Wesentliche Einrichtungen ***sollten*** deshalb einem vollständigen Aufsichtssystem (***ex-ante*** und ***ex-post***) und wichtige Einrichtungen einem vereinfachten Aufsichtssystem (nur ***ex-post***) unterliegen. Im letzteren Fall bedeutet dies, dass wichtige Einrichtungen die Erfüllung der Anforderungen an das Cybersicherheitsrisikomanagement nicht

Geänderter Text

(70) Zur Stärkung der Aufsichtsbefugnisse und der Maßnahmen, die zu einer wirksamen Befolgung der Vorschriften beitragen, ***und zur Erreichung eines hohen gemeinsamen Sicherheitsniveaus im gesamten digitalen Sektor, unter anderem durch die Prävention von Risiken für Nutzer oder andere Netze, Informationssysteme und Dienste,*** sollte diese Richtlinie einen Mindestumfang an Aufsichtsmaßnahmen und -mitteln vorsehen, mit welchen die zuständigen Behörden wesentliche und wichtige Einrichtungen beaufsichtigen können. Darüber hinaus sollte in dieser Richtlinie eine Abgrenzung zwischen den Aufsichtssystemen für wesentliche und für wichtige Einrichtungen vorgenommen werden, um die Verpflichtungen sowohl für die Einrichtungen als auch für die zuständigen Behörden ausgewogen zu gestalten. ***Unter Berücksichtigung eines risikobasierten Ansatzes sollten*** wesentliche Einrichtungen deshalb einem vollständigen Aufsichtssystem (***ex ante***

systematisch zu dokumentieren hätten und die zuständigen Behörden ein reaktives Ex-post-Aufsichtskonzept anwenden und nicht generell verpflichtet sein sollten, diese Einrichtungen zu beaufsichtigen.

und ***ex post***) und wichtige Einrichtungen einem vereinfachten Aufsichtssystem (nur ***ex post***) unterliegen. Im letzteren Fall bedeutet dies, dass wichtige Einrichtungen die Erfüllung der Anforderungen an das Cybersicherheitsrisikomanagement nicht systematisch zu dokumentieren hätten und die zuständigen Behörden ein reaktives Ex-post-Aufsichtskonzept anwenden und ***somit*** nicht generell verpflichtet sein sollten, diese Einrichtungen zu beaufsichtigen***, es sei denn, es liegt nachweislich eine Pflichtverletzung vor***.

Änderungsantrag 38
Vorschlag für eine Richtlinie
Erwägung 76

Vorschlag der Kommission	*Geänderter Text*
(76) Um die Wirksamkeit und Abschreckungskraft der Sanktionen bei Verstößen gegen die Verpflichtungen aus dieser Richtlinie zu erhöhen, sollten die zuständigen Behörden befugt sein, Sanktionen zu verhängen, die darin bestehen, die Zertifizierung oder Genehmigung für ***einen Teil oder alle*** von einer wesentlichen Einrichtung erbrachten Dienste auszusetzen ***und natürlichen Personen die Ausübung von Leitungsaufgaben vorübergehend zu untersagen***. Angesichts ihrer Schwere und ihrer Auswirkungen auf die Tätigkeiten der Einrichtungen und letztlich auf ihre Verbraucher sollten solche Sanktionen im Verhältnis zur Schwere des Verstoßes und unter Berücksichtigung der besonderen Umstände des Einzelfalls verhängt werden; hierzu zählen auch die Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, sowie die zur Verhinderung oder Minderung des erlittenen Schadens und/oder der erlittenen Verluste ergriffenen Maßnahmen. Solche Sanktionen sollten nur als äußerstes Mittel verhängt werden, also erst nachdem die anderen einschlägigen Durchsetzungsmaßnahmen nach dieser	(76) Um die Wirksamkeit und Abschreckungskraft der Sanktionen bei Verstößen gegen die Verpflichtungen aus dieser Richtlinie zu erhöhen, sollten die zuständigen Behörden befugt sein, Sanktionen zu verhängen, die darin bestehen, die Zertifizierung oder Genehmigung für ***die*** von einer wesentlichen Einrichtung erbrachten ***einschlägigen*** Dienste auszusetzen. Angesichts ihrer Schwere und ihrer Auswirkungen auf die Tätigkeiten der Einrichtungen und letztlich auf ihre Verbraucher sollten solche Sanktionen im Verhältnis zur Schwere des Verstoßes und unter Berücksichtigung der besonderen Umstände des Einzelfalls verhängt werden; hierzu zählen auch die Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, sowie die zur Verhinderung oder Minderung des erlittenen Schadens und/oder der erlittenen Verluste ergriffenen Maßnahmen. Solche Sanktionen sollten nur als äußerstes Mittel verhängt werden, also erst nachdem die anderen einschlägigen Durchsetzungsmaßnahmen nach dieser Richtlinie ausgeschöpft wurden, und nur so lange, bis die betroffenen Einrichtungen

Richtlinie ausgeschöpft wurden, und nur so lange, bis die betroffenen Einrichtungen die erforderlichen Maßnahmen zur Behebung der Mängel ergreifen oder die Anforderungen der zuständigen Behörde, auf die sich die Sanktionen beziehen, erfüllen. Für die Verhängung solcher Sanktionen muss es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta der Grundrechte der Europäischen Union, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, der Unschuldsvermutung und des Rechts auf Verteidigung, entsprechen.

die erforderlichen Maßnahmen zur Behebung der Mängel ergreifen oder die Anforderungen der zuständigen Behörde, auf die sich die Sanktionen beziehen, erfüllen. Für die Verhängung solcher Sanktionen muss es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta der Grundrechte der Europäischen Union, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, der Unschuldsvermutung und des Rechts auf Verteidigung, entsprechen.

Änderungsantrag 39
Vorschlag für eine Richtlinie
Erwägung 79

Vorschlag der Kommission	*Geänderter Text*
(79) Es sollte ein Peer-Review-Mechanismus eingeführt werden, der es ermöglicht, dass von den Mitgliedstaaten benannte Sachverständige die Umsetzung der Cybersicherheitsstrategien, einschließlich der Kapazitäten der Mitgliedstaaten und der verfügbaren Ressourcen, einer Bewertung unterziehen.	(79) Es sollte ein Peer-Review-Mechanismus eingeführt werden, der es ermöglicht, dass von den Mitgliedstaaten ***und der ENISA*** benannte Sachverständige die Umsetzung der Cybersicherheitsstrategien, einschließlich der Kapazitäten der Mitgliedstaaten und der verfügbaren Ressourcen, einer Bewertung unterziehen ***und dass bewährte Verfahren ausgetauscht werden***.

Änderungsantrag 40
Vorschlag für eine Richtlinie
Erwägung 80

Vorschlag der Kommission	*Geänderter Text*
(80) Um neuen Cyberbedrohungen, technologischen Entwicklungen oder sektorspezifischen Eigenschaften Rechnung zu tragen, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV	(80) Um neuen Cyberbedrohungen, technologischen Entwicklungen oder sektorspezifischen Eigenschaften Rechnung zu tragen, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV

Rechtsakte in Bezug auf Elemente zu erlassen, die die in dieser Richtlinie vorgeschriebenen Risikomanagementmaßnahmen betreffen. Der Kommission sollte ***auch*** die Befugnis übertragen werden, delegierte Rechtsakte zu erlassen, in denen festgelegt wird, ***welche Kategorien wesentlicher*** Einrichtungen ***ein Zertifikat erlangen müssen und welche spezifischen europäischen Schemata für die Cybersicherheitszertifizierung dabei anzuwenden*** sind. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung[26] niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, 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 Vorbereitung der delegierten Rechtsakte befasst sind.	Rechtsakte in Bezug auf Elemente zu erlassen, die die in dieser Richtlinie vorgeschriebenen Risikomanagementmaßnahmen betreffen. Der Kommission sollte ***die Befugnis übertragen werden, delegierte Rechtsakte zur Festlegung der technischen Elemente im Zusammenhang mit den Risikomanagementmaßnahmen zu erlassen. Der Kommission sollte ferner*** die Befugnis übertragen werden, delegierte Rechtsakte zu erlassen, in denen ***die Art der Informationen*** festgelegt wird, ***die von wesentlichen und bedeutenden*** Einrichtungen ***über alle Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Erbringung ihrer Dienste haben, oder über Beinahe-Vorfälle zu übermitteln*** sind***, und in denen festgelegt wird, in welchen Fällen ein Sicherheitsvorfall als erheblich zu betrachten ist***. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung[26] niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, 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 Vorbereitung der delegierten Rechtsakte befasst sind.
[26] ABl. L 123 vom 12.5.2016, S. 1.	[26] ABl. L 123 vom 12.5.2016, S. 1.

Änderungsantrag 41
Vorschlag für eine Richtlinie
Erwägung 81

Vorschlag der Kommission	*Geänderter Text*
(81) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung der einschlägigen Bestimmungen dieser Richtlinie in Bezug auf die Verfahrensmodalitäten, die für das Funktionieren der Kooperationsgruppe erforderlich sind, ***die technischen Elemente im Zusammenhang mit Risikomanagementmaßnahmen oder die Art der Informationen,*** das Format und das Verfahren für die Meldung von Sicherheitsvorfällen, sollten der Kommission Durchführungsbefugnisse übertragen werden. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates[27] ausgeübt werden.	(81) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung der einschlägigen Bestimmungen dieser Richtlinie in Bezug auf die Verfahrensmodalitäten, die für das Funktionieren der Kooperationsgruppe erforderlich sind, das Format und das Verfahren für die Meldung von Sicherheitsvorfällen, sollten der Kommission Durchführungsbefugnisse übertragen werden. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates[27] ausgeübt werden.
[27] 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).	[27] 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).

Änderungsantrag 42
Vorschlag für eine Richtlinie
Artikel 1 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Mit dieser Richtlinie werden Maßnahmen festgelegt, mit denen in der Union ein hohes gemeinsames Cybersicherheitsniveau sichergestellt werden soll.	(1) Mit dieser Richtlinie werden Maßnahmen festgelegt, mit denen in der Union ein hohes gemeinsames Cybersicherheitsniveau sichergestellt werden soll***, um ein vertrauenswürdiges digitales Umfeld für Verbraucher und Wirtschaftsbeteiligte zu schaffen und das Funktionieren des Binnenmarkts zu verbessern und Hindernisse im***

	Zusammenhang mit dem Funktionieren des Binnenmarkts zu beseitigen.

Änderungsantrag 43
Vorschlag für eine Richtlinie
Artikel 2 – Absatz 2 – Unterabsatz 1 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(2) Unabhängig von der Größe der Einrichtungen gilt diese Richtlinie jedoch auch für ***die*** in den Anhängen I und II genannten ***Einrichtungen***, wenn	(2) Unabhängig von der Größe der Einrichtungen gilt diese Richtlinie jedoch auch für ***Einrichtungen der*** in den Anhängen I und II genannten ***Art***, wenn

Änderungsantrag 44
Vorschlag für eine Richtlinie
Artikel 2 – Absatz 2 – Unterabsatz 2 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	Die Kommission gibt Leitlinien heraus, um die Mitgliedstaaten bei der ordnungsgemäßen Umsetzung der Bestimmungen über den Anwendungsbereich zu unterstützen und etwaige Ausnahmen für bestimmte wichtige Einrichtungen vom Anwendungsbereich der Richtlinie oder von einigen ihrer Bestimmungen zu gewähren, wobei in Bezug auf die Einrichtungen ihr geringer Grad der Kritikalität in ihrem spezifischen Sektor und/oder ihr geringer Grad der Abhängigkeit von anderen Sektoren oder Arten von Diensten berücksichtigt wird bzw. werden. Die Mitgliedstaaten teilen der Kommission unter umfassender Berücksichtigung der Leitlinien der Kommission ihre diesbezüglichen begründeten Beschlüsse mit.

Änderungsantrag 45
Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 4

Vorschlag der Kommission	*Geänderter Text*
4. „nationale Cybersicherheitsstrategie“ einen kohärenten Rahmen eines Mitgliedstaats mit strategischen Zielen und Prioritäten für die Sicherheit von Netz- und Informationssystemen in diesem Mitgliedstaat;	4. „nationale Cybersicherheitsstrategie“ einen kohärenten Rahmen eines Mitgliedstaats mit strategischen Zielen und Prioritäten für die Sicherheit von Netz- und Informationssystemen in diesem Mitgliedstaat ***sowie die zu ihrer Verwirklichung erforderlichen Maßnahmen***;

Änderungsantrag 46
Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 5 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	5a. „grenzüberschreitender Sicherheitsvorfall“ jeden Sicherheitsvorfall, der Betreiber unter der Aufsicht zuständiger nationaler Behörden aus mindestens zwei verschiedenen Mitgliedstaaten betrifft;

Änderungsantrag 47
Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 6 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	6a. „Beinahe-Vorfall“ ein Ereignis, das das Potenzial gehabt hätte, Schäden zu verursachen, dessen vollständiger Eintritt jedoch verhindert wurde;

Änderungsantrag 48
Vorschlag für eine Richtlinie
Artikel 4 – Absatz 1 – Nummer 15 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	15a. „Domänennamen-Registrierungsdienste“ Dienste, die von

	Domänennamen-Registern und Domänennamen-Registrierungsstellen, Anbietern von Datenschutz- oder Proxy-Registrierungsdiensten, Domänenmaklern oder Wiederverkäufern erbracht werden, sowie alle anderen Dienste, die mit der Registrierung von Domänennamen zusammenhängen;

Änderungsantrag 49
Vorschlag für eine Richtlinie
Artikel 5 – Absatz 1 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(1) Jeder Mitgliedstaat verabschiedet eine nationale Cybersicherheitsstrategie, in der die strategischen Ziele sowie angemessene politische und regulatorische Maßnahmen zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus festgelegt werden. Die nationale Cybersicherheitsstrategie muss insbesondere Folgendes umfassen:	(1) Jeder Mitgliedstaat verabschiedet eine nationale Cybersicherheitsstrategie, in der die strategischen Ziele sowie angemessene politische und regulatorische Maßnahmen***, einschließlich angemessener personeller und finanzieller Ressourcen,*** zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus festgelegt werden. Die nationale Cybersicherheitsstrategie muss insbesondere Folgendes umfassen:

Änderungsantrag 50
Vorschlag für eine Richtlinie
Artikel 5 – Absatz 1 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) einen Steuerungsrahmen zur Verwirklichung dieser Ziele und Prioritäten, der die in Absatz 2 genannten Konzepte sowie die Aufgaben und Zuständigkeiten öffentlicher Stellen und Einrichtungen sowie anderer relevanter Akteure umfasst;	b) einen Steuerungsrahmen zur Verwirklichung dieser Ziele und Prioritäten, der die in Absatz 2 genannten Konzepte sowie die Aufgaben und Zuständigkeiten öffentlicher Stellen und Einrichtungen sowie anderer relevanter Akteure umfasst***, einschließlich der für Cyberaufklärung und Cyberabwehr zuständigen Stellen***;

Änderungsantrag 51
Vorschlag für eine Richtlinie
Artikel 5 – Absatz 1 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) eine Bewertung zur Ermittlung von relevanten Anlagen und Cybersicherheitsrisiken in diesem Mitgliedstaat;	c) eine Bewertung zur Ermittlung von relevanten Anlagen und Cybersicherheitsrisiken in diesem Mitgliedstaat***, einschließlich potenzieller Engpässe, die sich negativ auf den Binnenmarkt auswirken können***;

Änderungsantrag 52
Vorschlag für eine Richtlinie
Artikel 5 – Absatz 1 – Buchstabe e

Vorschlag der Kommission	*Geänderter Text*
e) eine Liste der verschiedenen Behörden und Akteure, die an der Umsetzung der nationalen Cybersicherheitsstrategie beteiligt sind;	e) eine Liste der verschiedenen Behörden und Akteure, die an der Umsetzung der nationalen Cybersicherheitsstrategie beteiligt sind***, einschließlich einer zentralen Anlaufstelle für KMU***;

Änderungsantrag 53
Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) Leitlinien für die Aufnahme und Spezifikation cybersicherheitsbezogener Anforderungen an IKT-Produkte und -Dienste bei der Vergabe öffentlicher Aufträge;	b) Leitlinien für die Aufnahme und Spezifikation cybersicherheitsbezogener Anforderungen an IKT-Produkte und -Dienste bei der Vergabe öffentlicher Aufträge***, einschließlich der Verwendung quelloffener Cybersicherheitsprodukte***;

Änderungsantrag 54
Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) ein Konzept zur Förderung und Erleichterung der koordinierten Offenlegung von Schwachstellen im Sinne des Artikels 6;	c) ein Konzept zur Förderung und Erleichterung der koordinierten Offenlegung von Schwachstellen im Sinne des Artikels 6***, unter anderem durch die Festlegung von Leitlinien und bewährten Verfahren auf der Grundlage bereits etablierter international anerkannter Standards für die Behandlung und Offenlegung von Schwachstellen***;

Änderungsantrag 55
Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe e

Vorschlag der Kommission	*Geänderter Text*
e) ein Konzept zur Förderung und ***Entwicklung von Cybersicherheitskompetenzen, Sensibilisierungsmaßnahmen*** sowie Forschungs- und Entwicklungsinitiativen;	e) ein Konzept zur Förderung ***der Cybersicherheit der Verbraucher, zur Sensibilisierung der Verbraucher für Cyberbedrohungen, zur Erhöhung der Cyberkompetenz, zur Stärkung des Vertrauens der Nutzer, der technologieneutralen Kompetenzen*** und ***der Bildung im Bereich der Cybersicherheit*** sowie ***zur Förderung von*** Forschungs- und Entwicklungsinitiativen ***und der Cybersicherheit von vernetzten Produkten***;

Änderungsantrag 56
Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe e a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ea) ein Konzept zur Förderung des Einsatzes von Kryptografie und Verschlüsselung, insbesondere durch KMU;

Änderungsantrag 57
Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe h

Vorschlag der Kommission	*Geänderter Text*
h) ein Konzept, das auf die spezifischen Bedürfnisse von KMU – ***insbesondere*** vom Anwendungsbereich dieser Richtlinie ***ausgenommener*** KMU – ausgerichtet ist und Orientierungshilfen sowie Unterstützung bei der Verbesserung ihrer Resilienz gegenüber Cybersicherheitsbedrohungen bietet.	h) ein Konzept, das ***die Cybersicherheit fördert und*** auf die spezifischen Bedürfnisse von KMU ***bei der Erfüllung der in dieser Richtlinie festgelegten Verpflichtungen sowie auf die besonderen Bedürfnisse der*** vom Anwendungsbereich dieser Richtlinie ***ausgenommenen*** KMU ausgerichtet ist und Orientierungshilfen sowie Unterstützung bei der Verbesserung ihrer Resilienz gegenüber Cybersicherheitsbedrohungen***, einschließlich beispielsweise Finanzierung und Ausbildung zur Unterstützung der Einführung von Cybersicherheitsmaßnahmen,*** bietet.

Änderungsantrag 58
Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe h a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ha) dieses Konzept umfasst die Einrichtung einer nationalen zentralen Anlaufstelle für KMU und einen Rahmen für die möglichst effiziente Nutzung der Zentren für digitale Innovation und der verfügbaren Mittel zur Erreichung der politischen Ziele;

Änderungsantrag 59
Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe h b (neu)

Vorschlag der Kommission	*Geänderter Text*
	hb) ein Konzept zur Förderung der kohärenten und auf Synergien abstellenden Nutzung der verfügbaren

Mittel;

Änderungsantrag 60
Vorschlag für eine Richtlinie
Artikel 5 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
(4) Die Mitgliedstaaten bewerten ihre nationalen Cybersicherheitsstrategien mindestens alle vier Jahre auf der Grundlage wesentlicher Leistungsindikatoren und ändern diese erforderlichenfalls. Die Agentur der Europäischen Union für Cybersicherheit (ENISA) unterstützt die Mitgliedstaaten auf Anfrage bei der Entwicklung einer nationalen Strategie und wesentlicher Leistungsindikatoren für die Bewertung der Strategie.	(4) Die Mitgliedstaaten bewerten ihre nationalen Cybersicherheitsstrategien mindestens alle vier Jahre auf der Grundlage wesentlicher Leistungsindikatoren und ändern diese erforderlichenfalls. Die Agentur der Europäischen Union für Cybersicherheit (ENISA) unterstützt die Mitgliedstaaten auf Anfrage bei der Entwicklung einer nationalen Strategie und wesentlicher Leistungsindikatoren für die Bewertung der Strategie. ***Die ENISA richtet ferner Empfehlungen an die Mitgliedstaaten zur Entwicklung wesentlicher Leistungsindikatoren für die Bewertung der nationalen Strategie, die auf EU-Ebene vergleichbar sind.***

Änderungsantrag 61
Vorschlag für eine Richtlinie
Artikel 6 – Überschrift

Vorschlag der Kommission	*Geänderter Text*
Koordinierte Offenlegung von Schwachstellen und ***europäisches Schwachstellenregister***	Koordinierte Offenlegung von Schwachstellen und ***eine europäische Schwachstellendatenbank***

Änderungsantrag 62
Vorschlag für eine Richtlinie
Artikel 6 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die ENISA entwickelt und pflegt ***ein europäisches Schwachstellenregister***. Zu diesem Zweck führt die ENISA	(2) Die ENISA entwickelt und pflegt ***eine europäische Schwachstellendatenbank***. Zu diesem

geeignete Informationssysteme, Konzepte und Verfahren ein und pflegt diese, damit insbesondere wichtige und wesentliche Einrichtungen sowie deren Anbieter von Netz- und Informationssystemen Schwachstellen in IKT-Produkten oder -Diensten offenlegen und registrieren können und allen interessierten Kreisen ***Zugang*** zu den im Register enthaltenen Informationen über Schwachstellen gewährt werden kann. ***Das Register muss*** insbesondere ***Folgendes umfassen:*** Informationen zur Beschreibung der Schwachstelle, des betroffenen IKT-Produkts oder der betroffenen IKT-Dienste sowie zum Ausmaß der Schwachstelle im Hinblick auf die Umstände, unter denen sie ausgenutzt werden kann, Informationen zur Verfügbarkeit entsprechender Patches und bei Nichtverfügbarkeit von Patches Orientierungshilfen für die Nutzer gefährdeter Produkte und Dienste, wie die von offengelegten Schwachstellen ausgehenden Risiken gemindert werden können.

Zweck führt die ENISA geeignete Informationssysteme, Konzepte und Verfahren ***sowie angemessene Maßnahmen zur Offenlegung*** ein und pflegt diese, damit insbesondere wichtige und wesentliche Einrichtungen sowie deren Anbieter von Netz- und Informationssystemen Schwachstellen in IKT-Produkten oder -Diensten offenlegen und ***auf einfache Weise*** registrieren können und allen interessierten Kreisen ***– unter der Voraussetzung, dass der Schutz der Privatsphäre und von Handelsgeheimnissen durch derartige Maßnahmen nicht untergraben wird – Zugang*** zu den im Register enthaltenen ***einschlägigen*** Informationen über Schwachstellen gewährt werden kann. ***Die Schwachstellendatenbank enthält*** insbesondere Informationen zur Beschreibung der Schwachstelle, des betroffenen IKT-Produkts oder der betroffenen IKT-Dienste sowie zum Ausmaß der Schwachstelle im Hinblick auf die Umstände, unter denen sie ausgenutzt werden kann, Informationen zur Verfügbarkeit entsprechender Patches und bei Nichtverfügbarkeit von Patches Orientierungshilfen für die Nutzer gefährdeter Produkte und Dienste, wie die von offengelegten Schwachstellen ausgehenden Risiken gemindert werden können. ***Um Doppelarbeit zu verhindern, schließt die ENISA eine Vereinbarung über den Informationsaustausch und eine Vereinbarung über die strukturierte Zusammenarbeit mit dem Register „Common Vulnerabilities and Exposures“ (Bekannte Schwachstellen und Anfälligkeiten) und gegebenenfalls mit anderen Datenbanken ab, die weltweit von vertrauenswürdigen Partnern entwickelt und gepflegt werden.***

Änderungsantrag 63
Vorschlag für eine Richtlinie
Artikel 7 – Absatz 1 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(1a) Benennt ein Mitgliedstaat mehr als eine zuständige Behörde gemäß Absatz 1, so gibt er eindeutig an, welche dieser zuständigen Behörden bei einem Sicherheitsvorfall oder einer Sicherheitskrise größeren Ausmaßes als Hauptanlaufstelle fungieren wird.

Änderungsantrag 64
Vorschlag für eine Richtlinie
Artikel 7 – Absatz 3 – Buchstabe f

Vorschlag der Kommission	*Geänderter Text*
f) die zwischen den einschlägigen nationalen Behörden und Stellen vereinbarten nationalen Verfahren und ***Regelungen***, die gewährleisten sollen, dass sich der Mitgliedstaat wirksam am koordinierten Management massiver Cybersicherheitsvorfälle und -krisen auf Unionsebene beteiligen und dieses unterstützen kann.	f) die zwischen den einschlägigen nationalen Behörden und Stellen vereinbarten nationalen Verfahren und ***die Koordinierung, einschließlich der für Cyberaufklärung und Cyberabwehr zuständigen Stellen***, die gewährleisten sollen, dass sich der Mitgliedstaat wirksam am koordinierten Management massiver Cybersicherheitsvorfälle und -krisen auf Unionsebene beteiligen und dieses unterstützen kann.

Änderungsantrag 65
Vorschlag für eine Richtlinie
Artikel 10 – Absatz 2 – Buchstabe d

Vorschlag der Kommission	*Geänderter Text*
d) dynamische Analyse von Risiken und Sicherheitsvorfällen sowie Lagebeurteilung im Hinblick auf die Cybersicherheit;	d) dynamische Analyse von Risiken und Sicherheitsvorfällen sowie Lagebeurteilung im Hinblick auf die Cybersicherheit***, auch durch die Analyse von Frühwarnungen und Meldungen gemäß Artikel 20***;

Änderungsantrag 66
Vorschlag für eine Richtlinie
Artikel 10 – Absatz 2 – Buchstabe e

Vorschlag der Kommission	*Geänderter Text*
e) auf Ersuchen einer Einrichtung Durchführung einer ***proaktiven*** Überprüfung der für die Bereitstellung ihrer Dienste verwendeten Netz- und Informationssysteme auf Schwachstellen (Schwachstellenscan);	e) auf Ersuchen einer Einrichtung Durchführung einer Überprüfung der für die Bereitstellung ihrer Dienste verwendeten Netz- und Informationssysteme auf Schwachstellen (Schwachstellenscan)***, um spezifische Bedrohungen zu erkennen, abzuschwächen oder zu verhindern***;

Änderungsantrag 67
Vorschlag für eine Richtlinie
Artikel 10 – Absatz 2 – Buchstabe f

Vorschlag der Kommission	*Geänderter Text*
f) Beteiligung am CSIRT-Netzwerk und auf Gegenseitigkeit beruhende Unterstützung anderer Mitglieder des Netzwerks auf deren Ersuchen**.**	f) ***aktive*** Beteiligung am CSIRT-Netzwerk und auf Gegenseitigkeit beruhende Unterstützung anderer Mitglieder des Netzwerks auf deren Ersuchen***;***

Änderungsantrag 68
Vorschlag für eine Richtlinie
Artikel 10 – Absatz 2 – Buchstabe f a (neu)

Vorschlag der Kommission	*Geänderter Text*
	fa) Bereitstellung operativer Unterstützung und Orientierungshilfe für die in den Anhängen I und II genannten Einrichtungen, insbesondere für KMU;

Änderungsantrag 69
Vorschlag für eine Richtlinie
Artikel 10 – Absatz 2 – Buchstabe f b (neu)

Vorschlag der Kommission	*Geänderter Text*
	fb) Teilnahme an gemeinsamen Cybersicherheitsübungen auf Unionsebene.

Änderungsantrag 70
Vorschlag für eine Richtlinie
Artikel 11 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Mitgliedstaaten stellen sicher, dass Meldungen von Sicherheitsvorfällen, erheblichen Cyberbedrohungen und Beinahe-Vorfällen gemäß dieser Richtlinie entweder ihren zuständigen Behörden oder ihren CSIRTs übermittelt werden. Entscheidet ein Mitgliedstaat, dass diese Meldungen nicht an seine CSIRTs zu richten sind, so wird den CSIRTs in dem zur Wahrnehmung ihrer Aufgaben erforderlichen Umfang Zugang zu den Daten über Sicherheitsvorfälle gewährt, die gemäß Artikel 20 von wesentlichen oder wichtigen Einrichtungen gemeldet werden.	(2) Die Mitgliedstaaten stellen sicher, dass Meldungen von Sicherheitsvorfällen, erheblichen Cyberbedrohungen und Beinahe-Vorfällen gemäß dieser Richtlinie entweder ihren zuständigen Behörden oder ihren CSIRTs übermittelt werden. Entscheidet ein Mitgliedstaat, dass diese Meldungen nicht an seine CSIRTs zu richten sind, so wird den CSIRTs in dem zur ***wirksamen*** Wahrnehmung ihrer Aufgaben erforderlichen Umfang ***ein angemessener*** Zugang zu den Daten über Sicherheitsvorfälle gewährt, die gemäß Artikel 20 von wesentlichen oder wichtigen Einrichtungen gemeldet werden.

Änderungsantrag 71
Vorschlag für eine Richtlinie
Artikel 11 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
(4) Soweit dies zur wirksamen Wahrnehmung der in dieser Richtlinie festgelegten Aufgaben und Pflichten erforderlich ist, sorgen die Mitgliedstaaten für eine angemessene Zusammenarbeit zwischen den zuständigen Behörden und den zentralen Anlaufstellen sowie den Strafverfolgungsbehörden, den Datenschutzbehörden, den gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] für kritische Infrastrukturen zuständigen Behörden und den gemäß der Verordnung (EU) XXXX/XXXX des Europäischen Parlaments und des Rates[39] [DORA-Verordnung] in dem jeweiligen Mitgliedstaat benannten nationalen Finanzbehörden.	(4) Soweit dies zur wirksamen Wahrnehmung der in dieser Richtlinie festgelegten Aufgaben und Pflichten erforderlich ist, sorgen die Mitgliedstaaten für eine angemessene Zusammenarbeit zwischen den zuständigen Behörden und den zentralen Anlaufstellen sowie den Strafverfolgungsbehörden, den Datenschutzbehörden, den gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] für kritische Infrastrukturen zuständigen Behörden und den gemäß der Verordnung (EU) XXXX/XXXX des Europäischen Parlaments und des Rates[39] [DORA-Verordnung] in dem jeweiligen Mitgliedstaat benannten nationalen Finanzbehörden ***sowie den für Cyberabwehr und Cyberaufklärung***

	zuständigen Behörden.
[39] [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].	[39] [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].

Änderungsantrag 72
Vorschlag für eine Richtlinie
Artikel 12 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Kooperationsgruppe nimmt ihre Aufgaben auf der Grundlage von zweijährlichen Arbeitsprogrammen gemäß Absatz 6 wahr.	(2) Die Kooperationsgruppe ***tritt regelmäßig zusammen und*** nimmt ihre Aufgaben auf der Grundlage von zweijährlichen Arbeitsprogrammen gemäß Absatz 6 wahr.

Änderungsantrag 73
Vorschlag für eine Richtlinie
Artikel 12 – Absatz 3 – Unterabsatz 2

Vorschlag der Kommission	*Geänderter Text*
Gegebenenfalls kann die Kooperationsgruppe Vertreter der maßgeblichen Interessenträger einladen, an ihren Arbeiten teilzunehmen.	Gegebenenfalls kann die Kooperationsgruppe Vertreter der maßgeblichen ***Einrichtungen und Agenturen der Union sowie*** Interessenträger einladen, an ihren Arbeiten teilzunehmen.

Änderungsantrag 74
Vorschlag für eine Richtlinie
Artikel 12 – Absatz 4 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) Bereitstellung von Orientierungshilfen für die zuständigen Behörden in Bezug auf die Umsetzung und Durchführung dieser Richtlinie;	a) Bereitstellung von Orientierungshilfen für die zuständigen Behörden in Bezug auf die Umsetzung und Durchführung dieser Richtlinie ***und Förderung ihrer einheitlichen Umsetzung in den Mitgliedstaaten***;

Änderungsantrag 75
Vorschlag für eine Richtlinie
Artikel 12 – Absatz 4 – Buchstabe a a (neu)

Vorschlag der Kommission	*Geänderter Text*
	aa) Austausch von Informationen über die politischen Prioritäten und die wichtigsten Herausforderungen im Bereich der Cybersicherheit sowie Festlegung der wichtigsten Ziele der Cybersicherheit;

Änderungsantrag 76
Vorschlag für eine Richtlinie
Artikel 12 – Absatz 4 – Buchstabe a b (neu)

Vorschlag der Kommission	*Geänderter Text*
	ab) Erörterung der nationalen Strategien der Mitgliedstaaten und ihrer Abwehrbereitschaft;

Änderungsantrag 77
Vorschlag für eine Richtlinie
Artikel 12 – Absatz 4 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) beratender Austausch und Zusammenarbeit mit der Kommission in Bezug auf neue politische Initiativen im Bereich der Cybersicherheit;	c) beratender Austausch und Zusammenarbeit mit der Kommission in Bezug auf neue politische Initiativen im Bereich der Cybersicherheit ***und mit dem Europäischen Auswärtigen Dienst hinsichtlich der geopolitischen Aspekte der Cybersicherheit in der Union***;

Änderungsantrag 78
Vorschlag für eine Richtlinie
Artikel 12 – Absatz 4 – Buchstabe f

Vorschlag der Kommission	*Geänderter Text*
f) Erörterung von Berichten über die in Artikel 16 Absatz 7 genannten Peer	f) Erörterung von Berichten über die in Artikel 16 Absatz 7 genannten Peer

Reviews;	Reviews***, Bewertung ihrer Funktionsweise und Ausarbeitung von Schlussfolgerungen und Empfehlungen***;

Änderungsantrag 79
Vorschlag für eine Richtlinie
Artikel 12 – Absatz 4 – Buchstabe k a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ka) Unterstützung der ENISA bei der Organisation gemeinsamer Schulungen für die zuständigen nationalen Behörden auf EU-Ebene.

Änderungsantrag 80
Vorschlag für eine Richtlinie
Artikel 12 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
(6) Die Kooperationsgruppe erstellt bis zum … [***24*** Monate nach Inkrafttreten dieser Richtlinie] und danach alle zwei Jahre ein Arbeitsprogramm mit den zur Umsetzung ihrer Ziele und Aufgaben zu ergreifenden Maßnahmen. Der Zeitrahmen des ersten gemäß dieser Richtlinie angenommenen Programms wird an den Zeitrahmen des letzten gemäß der Richtlinie (EU) 2016/1148 angenommenen Programms angepasst.	(6) Die Kooperationsgruppe erstellt bis zum … [***12*** Monate nach Inkrafttreten dieser Richtlinie] und danach alle zwei Jahre ein Arbeitsprogramm mit den zur Umsetzung ihrer Ziele und Aufgaben zu ergreifenden Maßnahmen. Der Zeitrahmen des ersten gemäß dieser Richtlinie angenommenen Programms wird an den Zeitrahmen des letzten gemäß der Richtlinie (EU) 2016/1148 angenommenen Programms angepasst.

Änderungsantrag 81
Vorschlag für eine Richtlinie
Artikel 12 – Absatz 8 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(8a) Die Kooperationsgruppe veröffentlicht regelmäßig einen zusammenfassenden Bericht über ihre Tätigkeiten unbeschadet der Vertraulichkeit der in ihren Sitzungen ausgetauschten Informationen.

Änderungsantrag 82
Vorschlag für eine Richtlinie
Artikel 13 – Absatz 3 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) Informationsaustausch zu den Kapazitäten der CSIRTs;	a) Informationsaustausch zu den Kapazitäten ***und der Abwehrbereitschaft*** der CSIRTs;

Änderungsantrag 83
Vorschlag für eine Richtlinie
Artikel 13 – Absatz 3 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) Austausch relevanter Informationen über Sicherheitsvorfälle, Beinahe-Vorfälle, Cyberbedrohungen, Risiken und Schwachstellen;	b) Austausch relevanter Informationen über Sicherheitsvorfälle, Beinahe-Vorfälle, Cyberbedrohungen, Risiken und Schwachstellen ***sowie Unterstützung der operativen Kapazitäten der Mitgliedstaaten***;

Änderungsantrag 84
Vorschlag für eine Richtlinie
Artikel 13 – Absatz 3 – Buchstabe d a (neu)

Vorschlag der Kommission	*Geänderter Text*
	da) Austausch und Erörterung von Informationen in Bezug auf grenzüberschreitende Sicherheitsvorfälle;

Änderungsantrag 85
Vorschlag für eine Richtlinie
Artikel 13 – Absatz 3 – Buchstabe g – Buchstabe i a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ia) Informationsaustausch;

Änderungsantrag 86
Vorschlag für eine Richtlinie
Artikel 13 – Absatz 3 – Buchstabe j

Vorschlag der Kommission	*Geänderter Text*
j) ***auf Antrag eines einzelnen CSIRT*** Erörterung der Fähigkeiten und der Abwehrbereitschaft ***dieses CSIRT***;	j) Erörterung der Fähigkeiten und der Abwehrbereitschaft ***von CSIRTs***;

Änderungsantrag 87
Vorschlag für eine Richtlinie
Artikel 13 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
(4) Für die Zwecke der Überprüfung gemäß Artikel 35 bewertet das CSIRT-Netzwerk bis zum □24 Monate nach Inkrafttreten dieser Richtlinie□ und danach ***alle zwei Jahre*** die Fortschritte bei der operativen Zusammenarbeit und erstellt einen Bericht. Der Bericht muss insbesondere Schlussfolgerungen zu den Ergebnissen der Peer Reviews gemäß Artikel 16 enthalten, die in Bezug auf nationale CSIRTs durchgeführt wurden, einschließlich der Schlussfolgerungen und Empfehlungen gemäß dem genannten Artikel. Dieser Bericht wird auch der Kooperationsgruppe übermittelt.	(4) Für die Zwecke der Überprüfung gemäß Artikel 35 bewertet das CSIRT-Netzwerk bis zum [24 Monate nach Inkrafttreten dieser Richtlinie] und danach ***jährlich*** die Fortschritte bei der operativen Zusammenarbeit und erstellt einen Bericht. Der Bericht muss insbesondere Schlussfolgerungen zu den Ergebnissen der Peer Reviews gemäß Artikel 16 enthalten, die in Bezug auf nationale CSIRTs durchgeführt wurden, einschließlich der Schlussfolgerungen und Empfehlungen gemäß dem genannten Artikel. Dieser Bericht wird auch der Kooperationsgruppe übermittelt.

Änderungsantrag 88
Vorschlag für eine Richtlinie
Artikel 14 – Absatz 3 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) Verbesserung der Vorsorge im Hinblick auf das Management massiver Sicherheitsvorfälle und Krisen;	a) Verbesserung der Vorsorge im Hinblick auf das Management massiver Sicherheitsvorfälle und Krisen***, einschließlich grenzüberschreitender Cyberbedrohungen***;

Änderungsantrag 89
Vorschlag für eine Richtlinie
Artikel 14 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
(5) EU-CyCLONe erstattet der Kooperationsgruppe regelmäßig Bericht über Cyberbedrohungen, Sicherheitsvorfälle und Trends, wobei der Schwerpunkt insbesondere auf deren Auswirkungen auf wesentliche und wichtige Einrichtungen liegt.	(5) EU-CyCLONe erstattet der Kooperationsgruppe regelmäßig Bericht über Cyberbedrohungen, Sicherheitsvorfälle und Trends, wobei der Schwerpunkt insbesondere auf deren Auswirkungen auf wesentliche und wichtige Einrichtungen ***und auf deren Resilienz*** liegt.

Änderungsantrag 90
Vorschlag für eine Richtlinie
Artikel 14 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
(6) EU-CyCLONe arbeitet auf der Grundlage vereinbarter Verfahrensmodalitäten mit dem CSIRT-Netzwerk zusammen.	(6) EU-CyCLONe arbeitet auf der Grundlage vereinbarter Verfahrensmodalitäten ***eng*** mit dem CSIRT-Netzwerk zusammen.

Änderungsantrag 91
Vorschlag für eine Richtlinie
Artikel 15 – Absatz 1 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(1) Die ENISA veröffentlicht in Zusammenarbeit mit der Kommission einen zweijährlichen Bericht über den Stand der Cybersicherheit in der Union. Dieser Bericht muss insbesondere Folgendes enthalten:	(1) Die ENISA veröffentlicht in Zusammenarbeit mit der Kommission einen zweijährlichen Bericht über den Stand der Cybersicherheit in der Union ***und legt ihn dem Europäischen Parlament vor***. Dieser Bericht muss insbesondere Folgendes enthalten:

Änderungsantrag 92
Vorschlag für eine Richtlinie
Artikel 15 – Absatz 1 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) eine Bewertung der Entwicklung von Cybersicherheitskapazitäten in der gesamten Union;	a) eine Bewertung der Entwicklung von Cybersicherheitskapazitäten in der gesamten Union***, einschließlich des allgemeinen Niveaus der Fähigkeiten und Kompetenzen im Bereich der Cybersicherheit, des allgemeinen Grads der Resilienz des Binnenmarkts gegenüber Cyberbedrohungen und des Grads der Umsetzung der Richtlinie in den Mitgliedstaaten***;

Änderungsantrag 93
Vorschlag für eine Richtlinie
Artikel 15 – Absatz 1 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) einen Cybersicherheitsindex für eine aggregierte Bewertung des Entwicklungsstands der Cybersicherheitskapazitäten**.**	c) einen Cybersicherheitsindex für eine aggregierte Bewertung des Entwicklungsstands der Cybersicherheitskapazitäten**,** ***einschließlich einer Gesamtbewertung der Cybersicherheit für Verbraucher;***

Änderungsantrag 94
Vorschlag für eine Richtlinie
Artikel 15 – Absatz 1 – Buchstabe c a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ca) die geopolitischen Aspekte, die sich direkt oder indirekt auf den Stand der Cybersicherheit in der Union auswirken.

Änderungsantrag 95
Vorschlag für eine Richtlinie
Artikel 16 – Absatz 1 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(1) Nach Konsultation der Kooperationsgruppe und der ENISA legt	(1) Nach Konsultation der Kooperationsgruppe und der ENISA legt

die Kommission spätestens ***18*** Monate nach Inkrafttreten dieser Richtlinie die Methode und den Inhalt eines Peer-Review-Systems zur Bewertung der Wirksamkeit der Cybersicherheitskonzepte der Mitgliedstaaten fest. Die Peer Reviews werden von technischen Sachverständigen für Cybersicherheit aus anderen als den überprüften Mitgliedstaaten durchgeführt und erstrecken sich mindestens auf Folgendes:	die Kommission spätestens ***12*** Monate nach Inkrafttreten dieser Richtlinie die Methode und den Inhalt eines Peer-Review-Systems zur Bewertung der Wirksamkeit der Cybersicherheitskonzepte der Mitgliedstaaten fest. Die Peer Reviews werden von technischen Sachverständigen für Cybersicherheit aus ***mindestens zwei*** anderen als den überprüften Mitgliedstaaten ***und der ENISA*** durchgeführt und erstrecken sich mindestens auf Folgendes:

Änderungsantrag 96
Vorschlag für eine Richtlinie
Artikel 16 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Methode muss objektive, nichtdiskriminierende, faire und transparente Kriterien umfassen, anhand deren die Mitgliedstaaten Sachverständige benennen, die für die Durchführung der Peer Reviews infrage kommen. Die ENISA und die Kommission benennen Sachverständige, die als Beobachter an den Peer Reviews teilnehmen. Die Kommission legt mit Unterstützung der ENISA im Rahmen der in Absatz 1 genannten Methode für jede Peer Review ein objektives, nichtdiskriminierendes, faires und transparentes System für die Auswahl und die Zufallszuweisung von Sachverständigen fest.	(2) Die Methode muss objektive, nichtdiskriminierende, ***technologieneutrale,*** faire und transparente Kriterien umfassen, anhand deren die Mitgliedstaaten Sachverständige benennen, die für die Durchführung der Peer Reviews infrage kommen. Die ENISA und die Kommission benennen Sachverständige, die als Beobachter an den Peer Reviews teilnehmen. Die Kommission legt mit Unterstützung der ENISA im Rahmen der in Absatz 1 genannten Methode für jede Peer Review ein objektives, nichtdiskriminierendes, faires und transparentes System für die Auswahl und die Zufallszuweisung von Sachverständigen fest.

Änderungsantrag 97
Vorschlag für eine Richtlinie
Artikel 18 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen ***geeignete und***	(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen technische und

verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen bei der Erbringung ihrer Dienste nutzen, zu beherrschen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist.

organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen bei der Erbringung ihrer Dienste nutzen, zu beherrschen. ***Diese Maßnahmen müssen für den Grad der Kritikalität des Sektors oder der Art des Dienstes sowie den Grad der Abhängigkeit der Einrichtung von anderen Sektoren oder Arten von Diensten geeignet und verhältnismäßig sein, und sie werden nach einer risikobasierten Bewertung erlassen.*** Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. ***Insbesondere sind Maßnahmen zu ergreifen, um die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste zu verhindern und so gering wie möglich zu halten.***

Änderungsantrag 98
Vorschlag für eine Richtlinie
Artikel 18 – Absatz 2 – Buchstabe d

Vorschlag der Kommission	*Geänderter Text*
d) ***Sicherheit*** der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren Anbietern oder Diensteanbietern beispielsweise Anbietern von Datenspeicher- und Datenverarbeitungsdiensten oder verwalteten Sicherheitsdiensten (MSS);	d) ***Maßnahmen zur Bewertung des Sicherheitsrisikos in*** der Lieferkette***,*** einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren Anbietern oder Diensteanbietern beispielsweise Anbietern von Datenspeicher- und Datenverarbeitungsdiensten oder verwalteten Sicherheitsdiensten (MSS);

Änderungsantrag 99
Vorschlag für eine Richtlinie
Artikel 18 – Absatz 2 – Buchstabe f

Vorschlag der Kommission	*Geänderter Text*
f) Konzepte und Verfahren (Erprobung und Prüfung) zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;	f) Konzepte und Verfahren (Erprobung und Prüfung) ***und regelmäßige Cybersicherheitsübungen*** zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;

Änderungsantrag 100
Vorschlag für eine Richtlinie
Artikel 18 – Absatz 2 – Buchstabe g

Vorschlag der Kommission	*Geänderter Text*
g) Einsatz von Kryptografie und ***Verschlüsselung.***	g) Einsatz von Kryptografie***,*** ***Verschlüsselung*** und ***insbesondere von Übermittlungsverschlüsselung;***

Änderungsantrag 101
Vorschlag für eine Richtlinie
Artikel 18 – Absatz 2 – Buchstabe g a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ga) Maßnahmen zur Sicherstellung einer angemessenen Schulung und Sensibilisierung im Bereich der Cybersicherheit.

Änderungsantrag 102
Vorschlag für eine Richtlinie
Artikel 18 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Die Mitgliedstaaten stellen sicher, dass die Einrichtungen bei der Erwägung geeigneter Maßnahmen nach Absatz 2 Buchstabe d die spezifischen Schwachstellen der einzelnen Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und	(3) Die Mitgliedstaaten stellen sicher, dass die Einrichtungen bei der Erwägung geeigneter Maßnahmen nach Absatz 2 Buchstabe d die spezifischen Schwachstellen der einzelnen Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und

Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, berücksichtigen.	Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, berücksichtigen***, sofern sie Zugang zu den einschlägigen Informationen haben***.

Änderungsantrag 103
Vorschlag für eine Richtlinie
Artikel 18 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
(5) ***Die*** Kommission ***kann Durchführungsrechtsakte*** erlassen, um die technischen und methodischen Spezifikationen für die in Absatz 2 genannten Elemente festzulegen***. Bei der Ausarbeitung dieser Rechtsakte verfährt die Kommission nach dem Prüfverfahren gemäß Artikel 37 Absatz 2 und beachtet dabei so weit wie möglich internationale und europäische Normen sowie die*** einschlägigen ***technischen Spezifikationen***.	(5) ***Der*** Kommission ***wird die Befugnis übertragen, delegierte Rechtsakte zu*** erlassen, um die technischen und methodischen Spezifikationen für die in Absatz 2 genannten Elemente festzulegen ***und dabei so weit wie möglich internationale und europäische Normen sowie die einschlägigen technischen Spezifikationen zu beachten. Bei der Ausarbeitung delegierter Rechtsakte konsultiert die Kommission auch alle einschlägigen Interessenträger.***

Änderungsantrag 104
Vorschlag für eine Richtlinie
Artikel 18 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
(6) ***Der*** Kommission ***wird die Befugnis übertragen, zur Ergänzung*** der ***in*** Absatz 2 ***genannten Elemente delegierte Rechtsakte gemäß Artikel 36 zu erlassen, um neuen Cyberbedrohungen, technologischen Entwicklungen oder sektorspezifischen Besonderheiten Rechnung zu tragen***.	(6) ***Die*** Kommission ***stellt in Zusammenarbeit mit der Kooperationsgruppe und der ENISA Leitlinien und bewährte Verfahren für die Einhaltung*** der ***Anforderungen nach*** Absatz 2 ***und insbesondere der Anforderung nach Buchstabe d des genannten Absatzes durch die Einrichtungen in angemessener Weise bereit***.

Änderungsantrag 105
Vorschlag für eine Richtlinie
Artikel 19 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) ***Die Kooperationsgruppe*** kann in Zusammenarbeit mit der Kommission und der ENISA koordinierte Risikobewertungen in Bezug auf die Sicherheit der Lieferketten bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte unter Berücksichtigung technischer und erforderlichenfalls nichttechnischer Risikofaktoren durchführen.	(1) ***Um das allgemeine Niveau der Cybersicherheit zu erhöhen,*** kann ***die Kooperationsgruppe*** in Zusammenarbeit mit der Kommission und der ENISA koordinierte Risikobewertungen in Bezug auf die Sicherheit der Lieferketten bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte unter Berücksichtigung technischer und erforderlichenfalls nichttechnischer Risikofaktoren***, wie etwa geopolitischer Risiken,*** durchführen.

Änderungsantrag 106
Vorschlag für eine Richtlinie
Artikel 20 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen den zuständigen Behörden oder dem CSIRT gemäß den Absätzen 3 und 4 unverzüglich jeden Sicherheitsvorfall ***melden***, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste hat. Gegebenenfalls unterrichten diese Einrichtungen die Empfänger ihrer Dienste unverzüglich über Sicherheitsvorfälle, die die Erbringung des jeweiligen Dienstes beeinträchtigen könnten. Die Mitgliedstaaten stellen sicher, dass diese Einrichtungen unter anderem alle Informationen übermitteln, die es den zuständigen Behörden oder dem CSIRT ermöglichen zu ermitteln, ob der Sicherheitsvorfall grenzübergreifende Auswirkungen hat.	(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen den zuständigen Behörden oder dem CSIRT gemäß den Absätzen 3 und 4 unverzüglich jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste hat***, oder jeden Beinahe-Vorfall melden***. Gegebenenfalls unterrichten diese Einrichtungen die Empfänger ihrer Dienste unverzüglich über Sicherheitsvorfälle, die die Erbringung des jeweiligen Dienstes beeinträchtigen könnten. Die Mitgliedstaaten stellen sicher, dass diese Einrichtungen unter anderem alle Informationen übermitteln, die es den zuständigen Behörden oder dem CSIRT ermöglichen zu ermitteln, ob der Sicherheitsvorfall ***oder der Beinahe-Vorfall*** grenzübergreifende Auswirkungen hat.

Änderungsantrag 107
Vorschlag für eine Richtlinie
Artikel 20 – Absatz 1 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(1a) Zur Vereinfachung der Meldepflichten richten die Mitgliedstaaten eine zentrale Anlaufstelle für alle Meldungen ein, die aufgrund dieser Richtlinie sowie anderer EU-Rechtsvorschriften wie der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG vorgeschrieben sind.

Änderungsantrag 108
Vorschlag für eine Richtlinie
Artikel 20 – Absatz 1 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	(1b) Die ENISA erstellt in Zusammenarbeit mit der Kooperationsgruppe mittels Leitlinien einheitliche Meldemuster, die die im Unionsrecht geforderten Informationen vereinfachen und straffen und den Befolgungsaufwand für die Unternehmen verringern.

Änderungsantrag 109
Vorschlag für eine Richtlinie
Artikel 20 – Absatz 2 – Unterabsatz 1

Vorschlag der Kommission	*Geänderter Text*
(2) ***Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen den zuständigen Behörden oder dem CSIRT unverzüglich jede von diesen Einrichtungen ermittelte erhebliche Cyberbedrohung melden, die nach deren Auffassung möglicherweise zu einem erheblichen Sicherheitsvorfall hätte führen können.***	***entfällt***

Änderungsantrag 110
Vorschlag für eine Richtlinie
Artikel 20 – Absatz 2 – Unterabsatz 2

Vorschlag der Kommission	*Geänderter Text*
Gegebenenfalls unterrichten diese Einrichtungen die potenziell von einer erheblichen Cyberbedrohung betroffenen Empfänger ihrer Dienste unverzüglich über alle Maßnahmen oder Abhilfemaßnahmen, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. Die Einrichtungen informieren diese Empfänger gegebenenfalls auch über die Bedrohung selbst. Mit der Meldung wird keine höhere Haftung der meldenden Einrichtung begründet.	***entfällt***

Änderungsantrag 111
Vorschlag für eine Richtlinie
Artikel 20 – Absatz 3 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) der Sicherheitsvorfall erhebliche Betriebsstörungen oder finanzielle Verluste für die betreffende Einrichtung verursacht hat ***oder potenziell verursachen könnte***;	a) der Sicherheitsvorfall erhebliche Betriebsstörungen oder finanzielle Verluste für die betreffende Einrichtung verursacht hat;

Änderungsantrag 112
Vorschlag für eine Richtlinie
Artikel 20 – Absatz 3 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) der Sicherheitsvorfall andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Verluste geschädigt hat ***oder potenziell schädigen könnte***.	b) der Sicherheitsvorfall andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Verluste geschädigt hat.

Änderungsantrag 113
Vorschlag für eine Richtlinie
Artikel 20 – Absatz 3 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(3a) Der Kommission wird die Befugnis übertragen, gemäß Artikel 36 delegierte Rechtsakte zu erlassen, um diese Richtlinie zu ergänzen, indem sie die Art der gemäß Absatz 1 des vorliegenden Artikels übermittelten Informationen festlegt und die Fälle, in denen ein Sicherheitsvorfall als erheblich im Sinne des Absatzes 3 des vorliegenden Artikels zu betrachten ist, näher bestimmt.

Änderungsantrag 114
Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Buchstabe -a (neu)

Vorschlag der Kommission	*Geänderter Text*
	-a) innerhalb von 24 Stunden nach Kenntnisnahme des Sicherheitsvorfalls eine Frühwarnung, ohne dass die betreffende Einrichtung verpflichtet ist, zusätzliche Informationen über den Vorfall offenzulegen;

Änderungsantrag 115
Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) unverzüglich, in jedem Fall aber innerhalb von ***24*** Stunden nach Kenntnisnahme des Sicherheitsvorfalls, eine erste Meldung, in der gegebenenfalls angegeben wird, ob der Sicherheitsvorfall vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist;	a) unverzüglich, in jedem Fall aber innerhalb von ***72*** Stunden nach Kenntnisnahme des Sicherheitsvorfalls, eine erste Meldung, in der gegebenenfalls angegeben wird, ob der Sicherheitsvorfall vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist;

Änderungsantrag 116
Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Buchstabe c – Einleitung

Vorschlag der Kommission	*Geänderter Text*
c) spätestens ***einen Monat*** nach Vorlage des Berichts gemäß Buchstabe a einen ***Abschlussbericht***, der mindestens Folgendes enthält:	c) spätestens ***drei Monate*** nach Vorlage des Berichts gemäß Buchstabe a einen ***umfassenden Bericht***, der mindestens Folgendes enthält:

Änderungsantrag 117
Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Buchstabe c – Buchstabe i

Vorschlag der Kommission	*Geänderter Text*
i) eine ***ausführliche*** Beschreibung des Sicherheitsvorfalls, seines Schweregrads und seiner Auswirkungen;	i) eine ***ausführlichere*** Beschreibung des Sicherheitsvorfalls, seines Schweregrads und seiner Auswirkungen;

Änderungsantrag 118
Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Buchstabe c a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ca) im Fall eines Sicherheitsvorfalls, der bei Vorlage des umfassenden Berichts gemäß Buchstabe c noch andauert, ist einen Monat nach der Bewältigung des Vorfalls ein Abschlussbericht vorzulegen.

Änderungsantrag 119
Vorschlag für eine Richtlinie
Artikel 20 – Absatz 7

Vorschlag der Kommission	*Geänderter Text*
(7) Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen Sicherheitsvorfall zu verhindern oder einen laufenden Sicherheitsvorfall zu bewältigen oder liegt die Offenlegung des Sicherheitsvorfalls anderweitig im	(7) Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen Sicherheitsvorfall zu verhindern oder einen laufenden Sicherheitsvorfall zu bewältigen oder liegt die Offenlegung des Sicherheitsvorfalls anderweitig im

öffentlichen Interesse, so ***können*** die zuständige Behörde oder das CSIRT sowie gegebenenfalls die Behörden oder die CSIRTs anderer betroffener Mitgliedstaaten nach Konsultation der betroffenen Einrichtung die Öffentlichkeit über den Sicherheitsvorfall ***informieren*** oder die Einrichtung ***auffordern***, dies zu tun.	öffentlichen Interesse, so ***informieren*** die zuständige Behörde oder das CSIRT sowie gegebenenfalls die Behörden oder die CSIRTs anderer betroffener Mitgliedstaaten nach Konsultation der betroffenen Einrichtung die Öffentlichkeit über den Sicherheitsvorfall oder ***fordern*** die Einrichtung ***auf***, dies zu tun.

Änderungsantrag 120
Vorschlag für eine Richtlinie
Artikel 20 – Absatz 8

Vorschlag der Kommission	*Geänderter Text*
(8) Auf Ersuchen der zuständigen Behörde oder des CSIRT leitet die zentrale Anlaufstelle die nach ***den Absätzen*** 1 ***und 2*** eingegangenen Meldungen an die zentralen Anlaufstellen der anderen betroffenen Mitgliedstaaten weiter.	(8) Auf Ersuchen der zuständigen Behörde oder des CSIRT leitet die zentrale Anlaufstelle die nach ***Absatz*** 1 eingegangenen Meldungen an die zentralen Anlaufstellen der anderen betroffenen Mitgliedstaaten weiter.

Änderungsantrag 121
Vorschlag für eine Richtlinie
Artikel 20 – Absatz 9

Vorschlag der Kommission	*Geänderter Text*
(9) Die zentrale Anlaufstelle legt der ENISA monatlich einen zusammenfassenden Bericht vor, der anonymisierte und aggregierte Daten zu Sicherheitsvorfällen, erheblichen Cyberbedrohungen und Beinahe-Vorfällen enthält, die gemäß ***den Absätzen*** 1 ***und 2*** und gemäß Artikel 27 gemeldet wurden. Um zur Bereitstellung vergleichbarer Informationen beizutragen, kann die ENISA technische Leitlinien zu den Parametern der in den zusammenfassenden Bericht aufzunehmenden Angaben herausgeben.	(9) Die zentrale Anlaufstelle legt der ENISA monatlich einen zusammenfassenden Bericht vor, der anonymisierte und aggregierte Daten zu Sicherheitsvorfällen, erheblichen Cyberbedrohungen und Beinahe-Vorfällen enthält, die gemäß ***Absatz*** 1 und gemäß Artikel 27 gemeldet wurden. Um zur Bereitstellung vergleichbarer Informationen beizutragen, kann die ENISA technische Leitlinien zu den Parametern der in den zusammenfassenden Bericht aufzunehmenden Angaben herausgeben.

Änderungsantrag 122
Vorschlag für eine Richtlinie
Artikel 20 – Absatz 10

Vorschlag der Kommission	*Geänderter Text*
(10) Die zuständigen Behörden stellen den gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannten zuständigen Behörden Informationen über Sicherheitsvorfälle und Cyberbedrohungen zur Verfügung, die nach ***den Absätzen*** 1 ***und 2*** von wesentlichen Einrichtungen, die im Sinne der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] als kritische Einrichtungen oder als kritischen Einrichtungen gleichwertige Einrichtungen gelten, gemeldet wurden.	(10) Die zuständigen Behörden stellen den gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannten zuständigen Behörden Informationen über Sicherheitsvorfälle und Cyberbedrohungen zur Verfügung, die nach ***Absatz*** 1 von wesentlichen Einrichtungen, die im Sinne der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] als kritische Einrichtungen oder als kritischen Einrichtungen gleichwertige Einrichtungen gelten, gemeldet wurden.

Änderungsantrag 123
Vorschlag für eine Richtlinie
Artikel 20 – Absatz 11

Vorschlag der Kommission	*Geänderter Text*
(11) Die Kommission kann Durchführungsrechtsakte erlassen, in denen die Art der Angaben, das Format und das Verfahren für Meldungen gemäß ***den Absätzen*** 1 ***und 2*** näher bestimmt werden. Die Kommission kann ferner Durchführungsrechtsakte erlassen, um genauer zu bestimmen, in welchen Fällen ein Sicherheitsvorfall als erheblich im Sinne des Absatzes 3 anzusehen ist. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 37 Absatz 2 genannten Prüfverfahren erlassen.	(11) Die Kommission kann Durchführungsrechtsakte erlassen, in denen die Art der Angaben, das Format und das Verfahren für Meldungen gemäß ***Absatz*** 1 näher bestimmt werden. Die Kommission kann ferner Durchführungsrechtsakte erlassen, um genauer zu bestimmen, in welchen Fällen ein Sicherheitsvorfall als erheblich im Sinne des Absatzes 3 anzusehen ist. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 37 Absatz 2 genannten Prüfverfahren erlassen.

Änderungsantrag 124
Vorschlag für eine Richtlinie
Artikel 21 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Die Mitgliedstaaten ***können*** wesentliche und wichtige Einrichtungen ***dazu verpflichten***, bestimmte IKT-Produkte, -Dienste und -Prozesse im Rahmen ***spezifischer*** europäischer Systeme für die Cybersicherheitszertifizierung, die gemäß Artikel 49 der Verordnung (EU) 2019/881 angenommen wurden, zertifizieren zu lassen, um die Erfüllung bestimmter in Artikel 18 genannter Anforderungen nachzuweisen***. Die zu zertifizierenden Produkte, Dienstleistungen*** und ***Prozesse können von einer wesentlichen oder wichtigen Einrichtung entwickelt oder von Dritten beschafft worden sein***.	(1) Die Mitgliedstaaten ***bestärken nach Konsultation der Kooperationsgruppe und der ENISA*** wesentliche und wichtige Einrichtungen ***darin***, bestimmte IKT-Produkte, -Dienste und -Prozesse***, die entweder von der wesentlichen oder wichtigen Einrichtung entwickelt oder von Dritten beschafft werden,*** im Rahmen europäischer Systeme für die Cybersicherheitszertifizierung, die gemäß Artikel 49 der Verordnung (EU) 2019/881 angenommen wurden, ***oder im Rahmen ähnlicher international anerkannter Zertifizierungssysteme*** zertifizieren zu lassen, um die Erfüllung bestimmter in Artikel 18 genannter Anforderungen nachzuweisen und ***das Cybersicherheitsniveau zu erhöhen. Wann immer dies möglich ist, fördern die Mitgliedstaaten die einheitliche Nutzung der angenommenen Zertifizierungssysteme***.

Änderungsantrag 125
Vorschlag für eine Richtlinie
Artikel 21 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) ***Der*** Kommission ***wird*** die ***Befugnis übertragen***, ***delegierte Rechtsakte zu erlassen, in denen ausgeführt wird***, welche Kategorien wesentlicher Einrichtungen ein Zertifikat ***erlangen müssen*** und welche spezifischen europäischen Systeme für die Cybersicherheitszertifizierung dabei nach Absatz 1 anzuwenden sind. ***Die delegierten Rechtsakte werden gemäß Artikel 36 erlassen.***	(2) ***Die*** Kommission ***bewertet regelmäßig*** die ***Effizienz und Nutzung der europäischen Systeme für die Cybersicherheitszertifizierung***, ***die gemäß Artikel 49 der Verordnung (EU) 2019/881 angenommen wurden, und ermittelt***, welche Kategorien wesentlicher Einrichtungen ***dazu aufgefordert werden müssen,*** ein Zertifikat ***zu erlangen,*** und welche spezifischen europäischen Systeme für die Cybersicherheitszertifizierung dabei nach Absatz 1 anzuwenden sind.

Änderungsantrag 126
Vorschlag für eine Richtlinie
Artikel 22 – Absatz -1 (neu)

Vorschlag der Kommission	*Geänderter Text*
	(-1) Die Kommission unterstützt und fördert in Zusammenarbeit mit der ENISA die Ausarbeitung und Durchsetzung von Normen, die von den einschlägigen Normungsgremien der Union sowie den internationalen Normungsgremien für die konvergente Umsetzung von Artikel 18 Absätze 1 und 2 festgelegt wurden. Die Kommission unterstützt die Aktualisierung der Normen im Lichte der technologischen Entwicklungen.

Änderungsantrag 127
Vorschlag für eine Richtlinie
Artikel 22 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Um die einheitliche Anwendung des Artikels 18 Absätze 1 und 2 zu gewährleisten, fördern die Mitgliedstaaten ohne Auferlegung oder willkürliche Bevorzugung der Verwendung einer bestimmten Technologieart die Anwendung europäischer oder international anerkannter Normen und Spezifikationen für die Sicherheit von Netz- und Informationssystemen.	(1) Um die einheitliche Anwendung des Artikels 18 Absätze 1 und 2 zu gewährleisten, fördern die Mitgliedstaaten ohne Auferlegung oder willkürliche Bevorzugung der Verwendung einer bestimmten Technologieart ***und gemäß den Leitlinien der ENISA und der Kooperationsgruppe*** die Anwendung europäischer oder international anerkannter Normen und Spezifikationen für die Sicherheit von Netz- und Informationssystemen.

Änderungsantrag 128
Vorschlag für eine Richtlinie
Artikel 23 – Titel

Vorschlag der Kommission	*Geänderter Text*
Datenbanken der Domänennamen und Registrierungsdaten	***Infrastruktur der*** Datenbanken der Domänennamen und Registrierungsdaten

Änderungsantrag 129
Vorschlag für eine Richtlinie
Artikel 23 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domänennamensystems zu leisten, stellen die Mitgliedstaaten sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, genaue und vollständige Domänennamen-Registrierungsdaten in einer eigenen Datenbank sammeln und pflegen, wobei die Datenschutzvorschriften der Union in Bezug auf personenbezogene Daten mit der gebotenen Sorgfalt zu beachten sind.	(1) Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domänennamensystems zu leisten, stellen die Mitgliedstaaten sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, genaue und vollständige Domänennamen-Registrierungsdaten***, die für die Erbringung ihrer Dienste erforderlich sind,*** in einer eigenen Datenbank sammeln***, überprüfen*** und pflegen, wobei die Datenschutzvorschriften der Union in Bezug auf personenbezogene Daten mit der gebotenen Sorgfalt zu beachten sind.

Änderungsantrag 130
Vorschlag für eine Richtlinie
Artikel 23 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Mitgliedstaaten stellen sicher, dass die ***Datenbanken*** zu den in Absatz 1 genannten Domänennamen-Registrierungsdaten einschlägige Angaben ***enthalten***, ***anhand derer*** die Inhaber der Domänennamen und die Kontaktstellen, die die Domänennamen im Rahmen der TLD verwalten, identifiziert und kontaktiert werden können.	(2) Die Mitgliedstaaten stellen sicher, dass die ***Datenbankinfrastruktur*** zu den in Absatz 1 genannten Domänennamen-Registrierungsdaten einschlägige Angaben ***enthält, die mindestens den Namen der Registrierten***, ***ihre Anschrift und E-Mail-Adresse sowie ihre Telefonnummer umfassen und die erforderlich sind, damit*** die Inhaber der Domänennamen und die Kontaktstellen, die die Domänennamen im Rahmen der TLD verwalten, identifiziert und kontaktiert werden können***, und zwar mindestens den Namen, die Anschrift, die E-Mail-Adresse und die Telefonnummer der Registrierten***.

Änderungsantrag 131
Vorschlag für eine Richtlinie
Artikel 23 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, über Vorgaben und Verfahren verfügen, mit denen sichergestellt wird, dass die ***Datenbanken*** genaue und vollständige Angaben ***enthalten***. Die Mitgliedstaaten stellen sicher, dass diese Vorgaben und Verfahren öffentlich zugänglich gemacht werden.	(3) Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, über Vorgaben und Verfahren verfügen, mit denen sichergestellt wird, dass die ***Datenbankinfrastruktur*** genaue***, überprüfte*** und vollständige Angaben ***enthält und dass unrichtige oder unvollständige Daten von dem Registrierten unverzüglich berichtigt oder gelöscht werden***. Die Mitgliedstaaten stellen sicher, dass diese Vorgaben und Verfahren öffentlich zugänglich gemacht werden.

Änderungsantrag 132
Vorschlag für eine Richtlinie
Artikel 23 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
(4) Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste ***für die TLD*** erbringen, unverzüglich nach der Registrierung eines Domänennamens ***die nicht personenbezogenen*** Domänenregistrierungsdaten veröffentlichen.	(4) Die Mitgliedstaaten stellen sicher, dass die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, unverzüglich nach der Registrierung eines Domänennamens ***und in jedem Fall innerhalb von 24 Stunden sämtliche*** Domänenregistrierungsdaten ***der juristischen Personen, die registriert sind,*** veröffentlichen.

Änderungsantrag 133
Vorschlag für eine Richtlinie
Artikel 23 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
(5) Die Mitgliedstaaten stellen sicher,	(5) Die Mitgliedstaaten stellen sicher,

dass ***die*** TLD-Register und ***die*** Einrichtungen, die Domänennamen-Registrierungsdienste ***für die TLD erbringen***, auf ***rechtmäßige und*** hinreichend begründete Anträge berechtigten Zugangsnachfragern im Einklang mit dem Datenschutzrecht der Union Zugang zu bestimmten Domänennamen-Registrierungsdaten gewähren. Die Mitgliedstaaten stellen sicher, dass ***die*** TLD-Register und ***die*** Einrichtungen, die Domänennamen-Registrierungsdienste ***für die TLD*** erbringen, alle Anträge auf Zugang unverzüglich beantworten. Die Mitgliedstaaten stellen sicher, dass die Vorgaben und Verfahren für die Offenlegung solcher Daten öffentlich zugänglich gemacht werden.	dass TLD-Register und Einrichtungen, die Domänennamen-Registrierungsdienste ***erbringen, verpflichtet sind***, auf hinreichend begründete Anträge berechtigten Zugangsnachfragern im Einklang mit dem Datenschutzrecht der Union Zugang zu bestimmten Domänennamen-Registrierungsdaten ***zu*** gewähren. Die Mitgliedstaaten stellen sicher, dass TLD-Register und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, alle ***rechtmäßigen und hinreichend begründeten*** Anträge auf Zugang unverzüglich ***und in jedem Fall innerhalb von 72 Stunden*** beantworten. Die Mitgliedstaaten stellen sicher, dass die Vorgaben und Verfahren für die Offenlegung solcher Daten öffentlich zugänglich gemacht werden.

Änderungsantrag 134
Vorschlag für eine Richtlinie
Artikel 24 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Für die Zwecke dieser Richtlinie wird davon ausgegangen, dass als Hauptniederlassung in der Union der in Absatz 1 genannten Einrichtungen jeweils die Niederlassung in demjenigen Mitgliedstaat gilt, in dem die Entscheidungen im Zusammenhang mit den Maßnahmen zum Cybersicherheitsrisikomanagement getroffen werden. Werden solche Entscheidungen in keiner Niederlassung in der Union getroffen, wird davon ausgegangen, dass sich die Hauptniederlassung der Einrichtung in dem Mitgliedstaat befindet, in dem die Niederlassung mit der höchsten Beschäftigtenzahl in der Union angesiedelt ist.	(2) Für die Zwecke dieser Richtlinie wird davon ausgegangen, dass als Hauptniederlassung in der Union der in Absatz 1 genannten Einrichtungen jeweils die Niederlassung in demjenigen Mitgliedstaat gilt, in dem die Entscheidungen im Zusammenhang mit den Maßnahmen zum Cybersicherheitsrisikomanagement getroffen werden. Werden solche Entscheidungen in keiner Niederlassung in der Union getroffen, wird davon ausgegangen, dass sich die Hauptniederlassung der Einrichtung in dem Mitgliedstaat befindet, in dem die Niederlassung mit der höchsten Beschäftigtenzahl in der Union angesiedelt ist. ***Dabei wird sichergestellt, dass die nationalen Regulierungsstellen nicht unverhältnismäßig belastet werden.***

Änderungsantrag 135
Vorschlag für eine Richtlinie
Artikel 25 – Absatz 1 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
(1) Die ENISA erstellt und pflegt ein Register wesentlicher und wichtiger Einrichtungen im Sinne des Artikels 24 Absatz 1. ***Die Einrichtungen*** übermitteln der ENISA spätestens bis zum … [12 Monate nach Inkrafttreten der Richtlinie] folgende Angaben:	(1) Die ENISA erstellt und pflegt ein Register wesentlicher und wichtiger Einrichtungen im Sinne des Artikels 24 Absatz 1. ***Zu diesem Zweck*** übermitteln ***die Einrichtungen*** der ENISA spätestens bis zum … [12 Monate nach Inkrafttreten der Richtlinie] folgende Angaben:

Änderungsantrag 136
Vorschlag für eine Richtlinie
Artikel 26 – Absatz 1 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) durch diesen Informationsaustausch das Cybersicherheitsniveau erhöht wird, insbesondere indem Aufklärungsarbeit über Cyberbedrohungen geleistet wird, die Fähigkeit solcher Bedrohungen, sich zu verbreiten eingedämmt bzw. verhindert wird und eine Reihe von Abwehrkapazitäten, die Beseitigung und Offenlegung von Schwachstellen, Techniken zur Erkennung von Bedrohungen, Eindämmungsstrategien oder Reaktions- und Wiederherstellungsphasen unterstützt werden.	b) durch diesen Informationsaustausch das Cybersicherheitsniveau erhöht wird, insbesondere indem Aufklärungsarbeit über Cyberbedrohungen geleistet wird, die Fähigkeit solcher Bedrohungen, sich zu verbreiten eingedämmt bzw. verhindert wird und eine Reihe von Abwehrkapazitäten, die Beseitigung und Offenlegung von Schwachstellen, Techniken zur Erkennung ***und Prävention*** von Bedrohungen, Eindämmungsstrategien oder Reaktions- und Wiederherstellungsphasen unterstützt werden.

Änderungsantrag 137
Vorschlag für eine Richtlinie
Artikel 26 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Die Mitgliedstaaten legen ***Vorschriften*** fest, in denen das Verfahren, die operativen Elemente (einschließlich der Nutzung spezieller IKT-Plattformen), der	(3) Die Mitgliedstaaten legen ***Leitlinien*** fest, in denen das Verfahren, die operativen Elemente (einschließlich der Nutzung spezieller IKT-Plattformen), der

Inhalt und die Bedingungen der in Absatz 2 genannten Vereinbarungen über den Informationsaustausch bestimmt werden. In diesen ***Vorschriften werden*** auch die Einzelheiten der Beteiligung von Behörden an solchen Vereinbarungen sowie operative Elemente, einschließlich der Nutzung spezieller IT-Plattformen, ***festgelegt***. Die Mitgliedstaaten unterstützen die Anwendung solcher Vereinbarungen im Einklang mit ihren in Artikel 5 Absatz 2 Buchstabe g genannten Konzepten.	Inhalt und die Bedingungen der in Absatz 2 genannten Vereinbarungen über den Informationsaustausch bestimmt werden. In diesen ***Leitlinien sind gegebenenfalls*** auch die Einzelheiten der Beteiligung von Behörden ***und unabhängigen Sachverständigen*** an solchen Vereinbarungen sowie operative Elemente, einschließlich der Nutzung spezieller IT-Plattformen, ***enthalten***. Die Mitgliedstaaten unterstützen die Anwendung solcher Vereinbarungen im Einklang mit ihren in Artikel 5 Absatz 2 Buchstabe g genannten Konzepten.

Änderungsantrag 138
Vorschlag für eine Richtlinie
Artikel 26 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
(5) Im Einklang mit dem Unionsrecht unterstützt die ENISA den Abschluss von Vereinbarungen über den Austausch von Informationen im Bereich der Cybersicherheit gemäß Absatz 2, indem sie bewährte Verfahren und Orientierungshilfen zur Verfügung stellt.	(5) Im Einklang mit dem Unionsrecht unterstützt die ENISA den Abschluss von Vereinbarungen über den Austausch von Informationen im Bereich der Cybersicherheit gemäß Absatz 2, indem sie bewährte Verfahren und Orientierungshilfen zur Verfügung stellt ***und den Informationsaustausch auf der Ebene der Union erleichtert und gleichzeitig geschäftssensible Daten schützt. Auf Ersuchen wesentlicher und wichtiger Einrichtungen wird die Kooperationsgruppe aufgefordert, bewährte Verfahren und Leitlinien bereitzustellen.***

Änderungsantrag 139
Vorschlag für eine Richtlinie
Artikel 27 – Absatz -1 (neu)

Vorschlag der Kommission	*Geänderter Text*
	(-1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen auf freiwilliger Basis

	Meldungen über von diesen Einrichtungen festgestellte Cyberbedrohungen übermitteln können, die zu einem erheblichen Sicherheitsvorfall hätten führen können. Die Mitgliedstaaten stellen sicher, dass die Einrichtungen für die Zwecke dieser Meldungen gemäß dem in Artikel 20 festgelegten Verfahren tätig werden. Freiwillige Meldungen dürfen nicht dazu führen, dass der meldenden Einrichtung zusätzliche Verpflichtungen auferlegt werden.

Änderungsantrag 140
Vorschlag für eine Richtlinie
Artikel 27 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
Die Mitgliedstaaten stellen sicher, dass unbeschadet von Artikel 3 Einrichtungen, die nicht in den Anwendungsbereich dieser Richtlinie fallen, auf freiwilliger Basis erhebliche Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle melden können. Bei der Bearbeitung dieser Meldungen werden die Mitgliedstaaten gemäß dem in Artikel 20 vorgesehenen Verfahren tätig. Die Mitgliedstaaten ***können*** Pflichtmeldungen vorrangig vor freiwilligen Meldungen ***bearbeiten***. Freiwillige Meldungen dürfen nicht dazu führen, dass der meldenden Einrichtung zusätzliche Verpflichtungen auferlegt werden, die nicht für sie gegolten hätten, wenn sie die Meldung nicht übermittelt hätte.	***(1)*** Die Mitgliedstaaten stellen sicher, dass unbeschadet von Artikel 3 Einrichtungen, die nicht in den Anwendungsbereich dieser Richtlinie fallen, auf freiwilliger Basis erhebliche Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle melden können. Bei der Bearbeitung dieser Meldungen werden die Mitgliedstaaten gemäß dem in Artikel 20 vorgesehenen Verfahren tätig. Die Mitgliedstaaten ***bearbeiten*** Pflichtmeldungen vorrangig vor freiwilligen Meldungen. Freiwillige Meldungen dürfen nicht dazu führen, dass der meldenden Einrichtung zusätzliche Verpflichtungen auferlegt werden, die nicht für sie gegolten hätten, wenn sie die Meldung nicht übermittelt hätte***; der betreffende Mitgliedstaat kann ihr jedoch Unterstützung durch die CSIRTs gewähren***.

Änderungsantrag 141
Vorschlag für eine Richtlinie
Artikel 28 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden die Einhaltung dieser Richtlinie, insbesondere der Verpflichtungen nach den Artikeln 18 und 20, wirksam überwachen und die erforderlichen Maßnahmen treffen.	(1) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden die Einhaltung dieser Richtlinie, insbesondere der Verpflichtungen nach den Artikeln 18 und 20, wirksam überwachen und die erforderlichen Maßnahmen treffen ***und für die Wahrnehmung ihrer Aufgaben angemessene Mittel erhalten***.

Änderungsantrag 142
Vorschlag für eine Richtlinie
Artikel 28 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Bei der Bearbeitung von Sicherheitsvorfällen, die zur Verletzung des Schutzes personenbezogener Daten führen, arbeiten die zuständigen Behörden eng mit den Datenschutzbehörden zusammen.	(2) Bei der Bearbeitung von Sicherheitsvorfällen, die zur Verletzung des Schutzes personenbezogener Daten führen, arbeiten die zuständigen Behörden eng mit den Datenschutzbehörden***, gegebenenfalls auch mit den Datenschutzbehörden anderer Mitgliedstaaten,*** zusammen.

Änderungsantrag 143
Vorschlag für eine Richtlinie
Artikel 29 – Absatz 2 – Buchstabe c

Vorschlag der Kommission	*Geänderter Text*
c) gezielte Sicherheitsprüfungen auf der Grundlage von Risikobewertungen oder verfügbaren risikobezogenen Informationen;	c) gezielte Sicherheitsprüfungen auf der Grundlage von Risikobewertungen oder verfügbaren risikobezogenen Informationen***, die von einer qualifizierten unabhängigen Stelle oder einer zuständigen Behörde durchgeführt werden***;

Änderungsantrag 144
Vorschlag für eine Richtlinie
Artikel 29 – Absatz 2 – Buchstabe f

Vorschlag der Kommission	*Geänderter Text*
f) Anforderung des Zugangs zu Daten, Dokumenten oder ***sonstigen*** Informationen, die zur Erfüllung ihrer Aufsichtsaufgaben erforderlich sind;	f) Anforderung des Zugangs zu ***einschlägigen*** Daten, Dokumenten oder Informationen, die zur Erfüllung ihrer Aufsichtsaufgaben erforderlich sind;

Änderungsantrag 145
Vorschlag für eine Richtlinie
Artikel 29 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Bei der Ausübung ihrer Befugnisse nach Absatz 2 Buchstaben e bis g geben die zuständigen Behörden den Zweck der Anfrage und die erbetenen Informationen an.	(3) Bei der Ausübung ihrer Befugnisse nach Absatz 2 Buchstaben e bis g geben die zuständigen Behörden den Zweck der Anfrage und die erbetenen Informationen an ***und beschränken ihre Anfragen auf den Umfang des Sicherheitsvorfalls bzw. des Umstands, der Anlass zur Sorge gibt***.

Änderungsantrag 146
Vorschlag für eine Richtlinie
Artikel 29 – Absatz 5 – Unterabsatz 1 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) die Zertifizierung oder Genehmigung für ***einen Teil oder alle*** von einer wesentlichen Einrichtung erbrachten Dienste oder Tätigkeiten auszusetzen oder eine Zertifizierungs- oder Genehmigungsstelle aufzufordern, die Zertifizierung oder Genehmigung auszusetzen;	a) die Zertifizierung oder Genehmigung für ***die maßgeblichen*** von einer wesentlichen Einrichtung erbrachten Dienste oder Tätigkeiten auszusetzen oder eine Zertifizierungs- oder Genehmigungsstelle aufzufordern, die Zertifizierung oder Genehmigung auszusetzen;

Änderungsantrag 147
Vorschlag für eine Richtlinie
Artikel 29 – Absatz 5 – Unterabsatz 1 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) gegen Personen, die auf Geschäftsführungs- bzw. Vorstandsebene	***entfällt***

oder Ebene des rechtlichen Vertreters Leitungsaufgaben in dieser wesentlichen Einrichtung wahrnehmen, und gegen jede andere natürliche Person, die für den Verstoß Verantwortung trägt, ein vorübergehendes Verbot zur Wahrnehmung von Leitungsaufgaben in dieser Einrichtung zu verhängen oder von den zuständigen Stellen oder Gerichten die Verhängung eines solchen Verbots zu verlangen.

Änderungsantrag 148
Vorschlag für eine Richtlinie
Artikel 30 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Werden Nachweise oder Hinweise dafür vorgelegt, dass eine wichtige Einrichtung ihren Verpflichtungen nach dieser Richtlinie, insbesondere den Artikeln 18 und 20, nicht nachkommt, so stellen die Mitgliedstaaten sicher, dass die zuständigen Behörden erforderlichenfalls im Wege von nachträglichen Aufsichtsmaßnahmen tätig werden.	(1) Werden Nachweise oder Hinweise dafür vorgelegt, dass eine wichtige Einrichtung ihren Verpflichtungen nach dieser Richtlinie, insbesondere den Artikeln 18 und 20, nicht nachkommt, so stellen die Mitgliedstaaten sicher, dass die zuständigen Behörden erforderlichenfalls ***und unter Berücksichtigung eines risikobasierten Ansatzes*** im Wege von nachträglichen Aufsichtsmaßnahmen tätig werden.

Änderungsantrag 149
Vorschlag für eine Richtlinie
Artikel 30 – Absatz 2 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
b) gezielte Sicherheitsprüfungen auf der Grundlage von Risikobewertungen oder verfügbaren risikobezogenen Informationen;	b) gezielte Sicherheitsprüfungen auf der Grundlage von Risikobewertungen oder verfügbaren risikobezogenen Informationen***, die von einer qualifizierten unabhängigen Stelle oder einer zuständigen Behörde durchgeführt werden***;

Änderungsantrag 150
Vorschlag für eine Richtlinie
Artikel 30 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Bei der Ausübung ihrer Befugnisse nach Absatz 2 Buchstabe d oder e geben die zuständigen Behörden den Zweck der Anfrage und die erbetenen Informationen an.	(3) Bei der Ausübung ihrer Befugnisse nach Absatz 2 Buchstabe d oder e geben die zuständigen Behörden den Zweck der Anfrage und die erbetenen Informationen an ***und beschränken ihre Anfragen auf den Umfang des Sicherheitsvorfalls bzw. des Umstands, der Anlass zur Sorge gibt***.

Änderungsantrag 151
Vorschlag für eine Richtlinie
Artikel 31 – Absatz 4

Vorschlag der Kommission	*Geänderter Text*
(4) Die Mitgliedstaaten stellen sicher, dass für Verstöße gegen die Verpflichtungen nach Artikel 18 oder Artikel 20 im Einklang mit den Absätzen 2 und 3 des vorliegenden Artikels Geldbußen mit einem Höchstbetrag von ***mindestens*** 10 000 000 EUR oder von bis zu 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wesentliche oder wichtige Einrichtung angehört, verhängt werden, je nachdem, welcher Betrag höher ist.	(4) Die Mitgliedstaaten stellen sicher, dass für Verstöße gegen die Verpflichtungen nach Artikel 18 oder Artikel 20 im Einklang mit den Absätzen 2 und 3 des vorliegenden Artikels Geldbußen mit einem Höchstbetrag von 10 000 000 EUR oder von bis zu 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wesentliche oder wichtige Einrichtung angehört, verhängt werden, je nachdem, welcher Betrag höher ist.

Änderungsantrag 152
Vorschlag für eine Richtlinie
Artikel 32 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Haben die zuständigen Behörden Hinweise darauf, dass der Verstoß einer wesentlichen oder wichtigen Einrichtung gegen die in den Artikeln 18 und 20 festgelegten Verpflichtungen eine Verletzung des Schutzes	(1) Haben die zuständigen Behörden Hinweise darauf, dass der Verstoß einer wesentlichen oder wichtigen Einrichtung gegen die in den Artikeln 18 und 20 festgelegten Verpflichtungen eine Verletzung des Schutzes

personenbezogener Daten im Sinne von Artikel 4 Absatz 12 der Verordnung (EU) 2016/679 zur Folge hat, die gemäß Artikel 33 der genannten Verordnung zu melden ist, unterrichten sie die gemäß den Artikeln 55 und 56 jener Verordnung zuständigen Aufsichtsbehörden innerhalb ***einer angemessenen Frist***.	personenbezogener Daten im Sinne von Artikel 4 Absatz 12 der Verordnung (EU) 2016/679 zur Folge hat, die gemäß Artikel 33 der genannten Verordnung zu melden ist, unterrichten sie die gemäß den Artikeln 55 und 56 jener Verordnung zuständigen Aufsichtsbehörden ***unverzüglich und in jedem Fall*** innerhalb ***von 72 Stunden***.

Änderungsantrag 153
Vorschlag für eine Richtlinie
Artikel 32 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) Ist die gemäß der Verordnung (EU) 2016/679 zuständige Aufsichtsbehörde in einem anderen Mitgliedstaat angesiedelt als die zuständige Behörde, so ***kann*** die zuständige Behörde die im selben Mitgliedstaat angesiedelte Aufsichtsbehörde davon in Kenntnis ***setzen***.	(3) Ist die gemäß der Verordnung (EU) 2016/679 zuständige Aufsichtsbehörde in einem anderen Mitgliedstaat angesiedelt als die zuständige Behörde, so ***setzt*** die zuständige Behörde ***auch*** die im selben Mitgliedstaat angesiedelte Aufsichtsbehörde davon in Kenntnis.

Änderungsantrag 154
Vorschlag für eine Richtlinie
Artikel 36 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 18 Absatz ***6*** und Artikel ***21*** Absatz ***2*** wird der Kommission für einen Zeitraum von fünf Jahren ab dem […] übertragen.	(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 18 Absatz ***5*** und Artikel ***20*** Absatz ***3*** wird der Kommission für einen Zeitraum von fünf Jahren ab dem […] übertragen.

Änderungsantrag 155
Vorschlag für eine Richtlinie
Artikel 36 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) ***Die Befugnisübertragung*** gemäß Artikel 18 Absatz ***6*** und Artikel ***21***	(3) ***Ein delegierter Rechtsakt, der*** gemäß Artikel 18 Absatz ***5*** und Artikel ***20***

Absatz ***2 kann vom Europäischen*** Parlament ***oder vom*** Rat ***jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind,*** wird ***von dem Beschluss über den Widerruf nicht berührt***.	Absatz ***3 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische*** Parlament ***noch der*** Rat ***innerhalb einer Frist von drei Monaten nach Übermittlung dieses 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. Auf Initiative des Europäischen Parlaments oder des Rates*** wird ***diese Frist um drei Monate verlängert***.

Änderungsantrag 156
Vorschlag für eine Richtlinie
Artikel 36 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
(6) Ein delegierter Rechtsakt, der gemäß Artikel 18 Absatz ***6*** und Artikel ***21*** Absatz ***2*** erlassen wurde, tritt 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 erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament ***und*** der Rat ***beide*** der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.	(6) Ein delegierter Rechtsakt, der gemäß Artikel 18 Absatz ***5*** und Artikel ***20*** Absatz ***3*** erlassen wurde, tritt 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 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. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.

ANLAGE: LISTE DER EINRICHTUNGEN UND PERSONEN, VON DENEN DER VERFASSER BEITRÄGE ERHALTEN HAT

Die folgende Liste wurde auf rein freiwilliger Basis und unter alleiniger Verantwortung des Verfassers erstellt. Der Verfasser erhielt bei der Ausarbeitung der Stellungnahme bis zu deren Annahme im Ausschuss Beiträge von folgenden Einrichtungen bzw. Personen:

Person	Einrichtung
	BSA (The Software Alliance)
	BusinessEurope
	Confederation of Danish Industries
	Danish Permanent Representation
	Deutsche Telekom
	Digital Europe
	DOT Europe
	ETNO (European Telecommunications Network Operators)
	French Permanent Representation
	German Permanent Representation
	HUAWEI
	IFPI
	INTEL
	ITI (The Information Technology Industry Council)
	Kaspersky
	MÆRSK
	Microsoft
	ICANN
	MOTION PICTURE ASSOCIATION
	Orgalim
	Palo Alto Networks

	Rettighedsalliancen

VERFAHREN DES MITBERATENDEN AUSSCHUSSES

Titel	Maßnahmen zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus in der Union, Aufhebung der Richtlinie (EU) 2016/1148
Bezugsdokumente – Verfahrensnummer	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Federführender Ausschuss Datum der Bekanntgabe im Plenum	ITRE 21.1.2021
Stellungnahme von Datum der Bekanntgabe im Plenum	IMCO 21.1.2021
Verfasser(in) der Stellungnahme Datum der Benennung	Morten Løkkegaard 9.2.2021
Prüfung im Ausschuss	26.5.2021 21.6.2021
Datum der Annahme	12.7.2021
Ergebnis der Schlussabstimmung	+: 42 –: 1 0: 2
Zum Zeitpunkt der Schlussabstimmung anwesende Mitglieder	Alex Agius Saliba, Andrus Ansip, Pablo Arias Echeverría, Alessandra Basso, Brando Benifei, Adam Bielan, Hynek Blaško, Biljana Borzan, Vlad-Marius Botoş, Markus Buchheit, Andrea Caroppo, Anna Cavazzini, Dita Charanzová, Deirdre Clune, David Cormand, Carlo Fidanza, Evelyne Gebhardt, Alexandra Geese, Sandro Gozi, Maria Grapini, Svenja Hahn, Virginie Joron, Eugen Jurzyca, Marcel Kolaja, Kateřina Konečná, Andrey Kovatchev, Jean-Lin Lacapelle, Maria-Manuel Leitão-Marques, Morten Løkkegaard, Antonius Manders, Leszek Miller, Anne-Sophie Pelletier, Miroslav Radačovský, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein, Marco Zullo
Zum Zeitpunkt der Schlussabstimmung anwesende Stellvertreter	Clara Aguilera, Maria da Graça Carvalho, Christian Doleschal, Claude Gruffat, Jiří Pospíšil, Kosma Złotowski

NAMENTLICHE SCHLUSSABSTIMMUNG IM MITBERATENDEN AUSSCHUSS

42	+
ECR	Adam Bielan, Carlo Fidanza, Kosma Złotowski
ID	Alessandra Basso, Hynek Blaško, Markus Buchheit, Virginie Joron, Jean-Lin Lacapelle
PPE	Pablo Arias Echeverría, Andrea Caroppo, Maria da Graça Carvalho, Deirdre Clune, Christian Doleschal, Andrey Kovatchev, Antonius Manders, Jiří Pospíšil, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein
Renew	Andrus Ansip, Vlad-Marius Botoş, Dita Charanzová, Sandro Gozi, Morten Løkkegaard, Marco Zullo
S&D	Alex Agius Saliba, Clara Aguilera, Brando Benifei, Biljana Borzan, Evelyne Gebhardt, Maria Grapini, Maria-Manuel Leitão-Marques, Leszek Miller, Christel Schaldemose
The Left	Kateřina Konečná, Anne-Sophie Pelletier
Verts/ALE	Anna Cavazzini, David Cormand, Alexandra Geese, Claude Gruffat, Marcel Kolaja

1	-
NI	Miroslav Radačovský

2	0
ECR	Eugen Jurzyca
Renew	Svenja Hahn

Erklärung der benutzten Zeichen:
+ : dafür
- : dagegen
0 : Enthaltung

14.7.2021

STELLUNGNAHME DES AUSSCHUSSES FÜR VERKEHR UND TOURISMUS

für den Ausschuss für Industrie, Forschung und Energie

zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Verfasser der Stellungnahme: Jakop G. Dalunde

KURZE BEGRÜNDUNG

Der Verkehrssektor wird immer anfälliger für Bedrohungen durch Cyberkriminalität und ist immer stärker von ihnen betroffen. Aufgrund seiner besonderen Merkmale weist der Sektor außerdem eine Reihe unterschiedlicher Schwachstellen auf. Die Änderungsanträge in diesem Entwurf einer Stellungnahme sind zwar eher allgemeiner Natur, diesen besonderen Gegebenheiten wurde jedoch Rechnung getragen. Die Vorschläge sind aus folgenden Gründen für den Verkehrssektor relevant:

- Beförderungen erfolgen häufig grenzüberschreitend, wobei zahlreiche Einrichtungen in die Zuständigkeit verschiedener Mitgliedstaaten fallen. Der Sektor ist aus diesem Grund beim Risikomanagement und bei den Meldepflichten im Bereich der Cybersicherheit in besonderem Maße von übermäßigen Unterschieden zwischen den einzelnen Mitgliedstaaten betroffen.

- Der Verkehrssektor ist auf einen sicheren Datenaustausch zwischen den verschiedenen Beteiligten angewiesen. Aufgrund der Vernetzung im Logistikbereich könnte eine unzureichende Cybersicherheit in einer Einrichtung das gesamte System gefährden und ernsthafte Konsequenzen für den Betrieb anderer Einrichtungen nach sich ziehen.

- Das Transportwesen ist eine arbeitsintensive Branche und daher besonders anfällig für Bedrohungen durch Cyberkriminalität, die auf Mitarbeiter abzielen.

Aus diesem Grund konzentrieren sich die Änderungsanträge auf folgende Themen: die Bewertung des Ausmaßes der Unterschiede bei den Verpflichtungen zur Cybersicherheit zwischen den Mitgliedstaaten, die Förderung der Angleichung dieser Verpflichtungen durch nicht legislative Maßnahmen, die Förderung von Mitarbeiterschulungen und des Erwerbs von Kenntnissen im Bereich der Cybersicherheitsrisiken.

Neben diesen allgemeinen Punkten ist anzumerken, dass bei der Erbringung von Transportdienstleistungen zunehmend auf internetfähige Fernsensoren zurückgegriffen wird und die Fahrzeuge immer stärker digitalisiert sind. Obwohl diese Geräte nicht unbedingt Teil der umfassenderen Informationssysteme sind, kann es erforderlich sein, sie speziellen Sicherheitsbewertungen zu unterwerfen.

ÄNDERUNGSANTRÄGE

Der Ausschuss für Verkehr und Tourismus ersucht den federführenden Ausschuss für Industrie, Forschung und Energie, folgende Änderungsanträge zu berücksichtigen:

Änderungsantrag 1
Vorschlag für eine Richtlinie
Erwägung 3

Vorschlag der Kommission	*Geänderter Text*
(3) Netz- und Informationssysteme sind durch den schnellen digitalen Wandel und die Vernetzung der Gesellschaft zu einem zentralen Bestandteil des Alltags und ***für*** den grenzüberschreitenden Austausch ***geworden***. Diese Entwicklung hat zu einer Ausweitung der Bedrohungslage im Bereich der Cybersicherheit geführt und neue Herausforderungen mit sich gebracht, die in allen Mitgliedstaaten entsprechende koordinierte und innovative Reaktionen erfordern. Die Anzahl, Tragweite, Komplexität, Häufigkeit und Auswirkungen von Cybersicherheitsvorfällen nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen dar. Im Ergebnis können Cybersicherheitsvorfälle die Ausübung wirtschaftlicher Tätigkeiten im Binnenmarkt beeinträchtigen, finanzielle Verluste verursachen, das Vertrauen der Nutzer ***untergraben*** und der Wirtschaft und Gesellschaft der Union großen Schaden zufügen. Heute sind daher im Bereich Cybersicherheit Vorsorge und Wirksamkeit wichtiger denn je für das reibungslose Funktionieren des Binnenmarkts.	(3) Netz- und Informationssysteme sind durch den schnellen digitalen Wandel und die Vernetzung der Gesellschaft zu einem zentralen Bestandteil des Alltags ***geworden*** und ***tragen zum Wachstum neuer Wirtschaftsmodelle und Dienste bei, zu denen etwa Modelle und Dienste im Zusammenhang mit der Gig-Economy, der On-Demand- und der Plattformwirtschaft gehören, und zwar auch mit Blick auf*** den grenzüberschreitenden Austausch ***und das Konzept „Mobilität als Dienstleistung“ (Mobility as a Service – MaaS)***. Diese Entwicklung hat zu einer Ausweitung der Bedrohungslage im Bereich der Cybersicherheit geführt und neue Herausforderungen mit sich gebracht, die in allen Mitgliedstaaten entsprechende koordinierte und innovative Reaktionen erfordern. Die Anzahl, Tragweite, Komplexität, Häufigkeit und Auswirkungen von Cybersicherheitsvorfällen nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen dar. Im Ergebnis können Cybersicherheitsvorfälle ***das Wohl der Gesellschaft schmälern,*** die Ausübung wirtschaftlicher Tätigkeiten im Binnenmarkt ***sowie sozialer Tätigkeiten*** beeinträchtigen, finanzielle Verluste verursachen, das Vertrauen der Nutzer und der ***Arbeitnehmer untergraben, der*** Wirtschaft und Gesellschaft der Union großen Schaden zufügen ***oder gar eine terroristische Bedrohung darstellen***. Heute sind daher im Bereich

	Cybersicherheit Vorsorge und Wirksamkeit wichtiger denn je für ***die Wahrung der Grundrechte und Grundfreiheiten in der Union und*** das reibungslose Funktionieren des Binnenmarkts. ***Darüber hinaus ist die Cybersicherheit für viele kritische Sektoren, wie etwa den Verkehrssektor, eine entscheidende Voraussetzung, um den digitalen Wandel erfolgreich zu bewältigen und die wirtschaftlichen, sozialen und dauerhaften Vorteile der Digitalisierung umfassend auszuschöpfen.***

Änderungsantrag 2

Vorschlag für eine Richtlinie
Erwägung 9

Vorschlag der Kommission	*Geänderter Text*
(9) Allerdings sollten auch Klein- und Kleinsteinrichtungen, die bestimmte Kriterien erfüllen, nach denen sie eine Schlüsselrolle für die Wirtschaft oder Gesellschaft des betreffenden Mitgliedstaats oder für bestimmte Sektoren oder Arten von Diensten spielen, von der vorliegenden Richtlinie erfasst werden. Die Mitgliedstaaten sollten für die Erstellung einer Liste solcher Einrichtungen zuständig sein und diese der Kommission übermitteln.	(9) Allerdings sollten auch Klein- und Kleinsteinrichtungen, die bestimmte Kriterien erfüllen, nach denen sie eine Schlüsselrolle für die Wirtschaft oder Gesellschaft des betreffenden Mitgliedstaats oder für bestimmte Sektoren oder Arten von Diensten spielen, von der vorliegenden Richtlinie erfasst werden. Die Mitgliedstaaten sollten für die Erstellung einer Liste solcher Einrichtungen zuständig sein und diese der Kommission übermitteln. ***Bei der Erstellung der Liste sollten die Besonderheiten von kleinen und mittleren Unternehmen (KMU) umfassend berücksichtigt werden, und es sollte darauf geachtet werden, dass KMU hierdurch kein übermäßiger Verwaltungsaufwand entsteht.***

Änderungsantrag 3

Vorschlag für eine Richtlinie
Erwägung 10

Vorschlag der Kommission	*Geänderter Text*
(10) Die Kommission kann in	(10) Die Kommission kann in

Zusammenarbeit mit der Kooperationsgruppe Leitlinien für die Anwendung der für ***Klein-*** und Kleinstunternehmen geltenden Kriterien herausgeben.	Zusammenarbeit mit der Kooperationsgruppe ***und einschlägigen Interessenträgern*** Leitlinien für die Anwendung der für ***kleine Unternehmen*** und Kleinstunternehmen geltenden Kriterien herausgeben. ***Die Kommission sollte außerdem dafür Sorge tragen, dass allen Kleinstunternehmen und kleinen Unternehmen, die in den Geltungsbereich dieser Richtlinie fallen, angemessene Orientierungshilfe zuteilwird. Die Kommission sollte mit Unterstützung der Mitgliedstaaten Kleinstunternehmen und kleinen Unternehmen Informationen diesbezüglich zukommen lassen.***

Änderungsantrag 4

Vorschlag für eine Richtlinie
Erwägung 12

Vorschlag der Kommission	*Geänderter Text*
(12) Durch sektorspezifische Rechtsvorschriften und Instrumente kann dazu beigetragen werden, ein hohes Maß an Cybersicherheit zu gewährleisten und gleichzeitig den Besonderheiten und Komplexitäten der Sektoren in vollem Umfang Rechnung zu tragen. Müssen wesentliche oder wichtige Einrichtungen gemäß einem sektorspezifischen Rechtsakt der Union Maßnahmen zum Cybersicherheitsrisikomanagement ergreifen oder Sicherheitsvorfälle oder erhebliche Cyberbedrohungen melden und ist dies in der Wirkung den in der vorliegenden Richtlinie festgelegten Verpflichtungen mindestens gleichwertig, so sollten diese sektorspezifischen Bestimmungen, einschließlich in Bezug auf Aufsicht und Durchsetzung, Anwendung finden. Die Kommission kann Leitlinien im Zusammenhang mit der Umsetzung der lex specialis herausgeben. Die vorliegende Richtlinie schließt nicht aus, dass zusätzliche sektorspezifische Rechtsakte der Union zu Maßnahmen zum Cybersicherheitsrisikomanagement und zur	(12) Durch sektorspezifische Rechtsvorschriften und Instrumente kann dazu beigetragen werden, ein hohes Maß an Cybersicherheit zu gewährleisten und gleichzeitig den Besonderheiten und Komplexitäten der Sektoren in vollem Umfang Rechnung zu tragen. Müssen wesentliche oder wichtige Einrichtungen gemäß einem sektorspezifischen Rechtsakt der Union Maßnahmen zum Cybersicherheitsrisikomanagement ergreifen oder Sicherheitsvorfälle oder erhebliche Cyberbedrohungen melden und ist dies in der Wirkung den in der vorliegenden Richtlinie festgelegten Verpflichtungen mindestens gleichwertig, so sollten diese sektorspezifischen Bestimmungen, einschließlich in Bezug auf Aufsicht und Durchsetzung, Anwendung finden. ***Um Rechtsunsicherheit bei der Auslegung und Anwendung dieser Richtlinie zu vermeiden, sollte die Kommission für Kohärenz zwischen dieser Richtlinie und den geltenden sektorspezifischen Rechtsvorschriften sorgen. Zu diesem Zweck sollte die***

Meldung von Sicherheitsvorfällen erlassen werden. ***Die vorliegende*** Richtlinie berührt nicht die bestehenden Durchführungsbefugnisse, die der Kommission in einer Reihe von Sektoren, darunter Verkehr und Energie, übertragen wurden.	***Kommission Überschneidungen und Redundanzen in den jeweiligen Rechtsvorschriften, rechtlichen Anforderungen oder Verfahren ermitteln, sodass sie beseitigt werden können.*** Die Kommission kann Leitlinien im Zusammenhang mit der Umsetzung der lex specialis herausgeben. Die vorliegende Richtlinie schließt nicht aus, dass zusätzliche sektorspezifische Rechtsakte der Union zu Maßnahmen zum Cybersicherheitsrisikomanagement und zur Meldung von Sicherheitsvorfällen erlassen werden. ***Diese*** Richtlinie berührt nicht die bestehenden Durchführungsbefugnisse, die der Kommission in einer Reihe von Sektoren, darunter Verkehr und Energie, übertragen wurden.

Änderungsantrag 5

Vorschlag für eine Richtlinie
Erwägung 15 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(15a) Die zunehmende Digitalisierung wichtiger Wirtschaftszweige wie zum Beispiel des Verkehrssektors sollte auf sichere Weise und mit eingebauter Resilienz erfolgen, um sicherzustellen, dass die gesamte Lieferkette angemessen auf Risiken und Bedrohungen reagiert. Daher bedarf es einer abgestimmten Vorgehensweise, die ein Mindestmaß an Sicherheit für vernetzte Geräte bietet, was insbesondere in Branchen wie dem Verkehr und in den Fällen gilt, in denen Geräte in Fahrzeuge eingebaut sind und standardmäßig eine Übermittlungsverschlüsselung verwenden.

Änderungsantrag 6

Vorschlag für eine Richtlinie
Erwägung 17

Vorschlag der Kommission	*Geänderter Text*
(17) Angesichts des Aufkommens innovativer Technologien und neuer ***Geschäftsmodelle*** dürften auf dem Markt neue Bereitstellungs- und Dienstmodelle für Cloud-Computing entstehen, um den sich wandelnden ***Kundenbedürfnissen*** gerecht zu werden. In diesem Zusammenhang können Cloud-Computing-Dienste in hochgradig verteilter Form, noch näher am Ort der Datengenerierung oder -sammlung, erbracht werden, wodurch vom traditionellen Modell zu einem hochgradig verteilten Modell („Edge-Computing“) übergegangen wird.	(17) Angesichts des Aufkommens innovativer Technologien ***wie etwa der künstlichen Intelligenz, neuer Geschäftsmodelle*** und neuer ***flexibler Telearbeitsmodelle*** dürften auf dem Markt neue Bereitstellungs- und Dienstmodelle für Cloud-Computing entstehen, um den sich wandelnden ***Bedürfnissen von Verbrauchern und Unternehmen*** gerecht zu werden. In diesem Zusammenhang können Cloud-Computing-Dienste in hochgradig verteilter Form, noch näher am Ort der Datengenerierung oder -sammlung, erbracht werden, wodurch vom traditionellen Modell zu einem hochgradig verteilten Modell („Edge-Computing“) übergegangen wird.

Änderungsantrag 7

Vorschlag für eine Richtlinie
Erwägung 18 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(18a) Da die Einführung autonomer Mobilität erhebliche Vorteile mit sich bringen wird, aber auch mit einer Reihe neuer Risiken verbunden ist – insbesondere in Bezug auf die Straßenverkehrssicherheit, die Cybersicherheit, die Rechte des geistigen Eigentums, Fragen im Zusammenhang mit dem Datenschutz und dem Datenzugriff, die technische Infrastruktur, die Normung und die Beschäftigung –, ist es von entscheidender Bedeutung, dafür zu sorgen, dass der Rechtsrahmen der Union diesen Herausforderungen angemessen Rechnung trägt und sämtliche Risiken für die Sicherheit von Netz- und Informationssystemen wirksam bewältigt.

Änderungsantrag 8

Vorschlag für eine Richtlinie
Erwägung 18 b (neu)

Vorschlag der Kommission	*Geänderter Text*
	(18b) Die Coronavirus-Pandemie hat gezeigt, wie wichtig es ist, die Union auf das digitale Jahrzehnt vorzubereiten und die Widerstandsfähigkeit gegenüber Cyberangriffen kontinuierlich zu verbessern. Daher zielt diese Richtlinie darauf ab, Mindestvorschriften für das Funktionieren des abgestimmten Rechtsrahmens festzulegen, um den digitalen Wandel sowie Innovationen in den Bereichen autonomer Verkehr, Logistik und Verkehrsmanagement bei allen Verkehrsträgern zu ermöglichen und bei den Nutzern, insbesondere Kleinstunternehmen, KMU und Start-ups, die Widerstandsfähigkeit gegenüber Cyberangriffen und die Möglichkeiten, Schwachstellen zu beheben, zu verbessern.

Änderungsantrag 9

Vorschlag für eine Richtlinie
Erwägung 19

Vorschlag der Kommission	*Geänderter Text*
(19) Anbieter von Postdiensten im Sinne der Richtlinie 97/67/EG des Europäischen Parlaments und des Rates[18] sowie Anbieter von Express- und Kurierdiensten sollten der vorliegenden Richtlinie unterliegen, wenn sie mindestens einen der Schritte in der Postzustellkette und insbesondere Abholung, Sortierung oder Zustellung, einschließlich Abholung durch den Empfänger, anbieten. ***Transportdienste***, die nicht in Verbindung mit einem dieser Schritte erbracht werden, sollten nicht unter Postdienste fallen.	(19) Anbieter von Postdiensten im Sinne der Richtlinie 97/67/EG des Europäischen Parlaments und des Rates[18] sowie Anbieter von Express- und Kurierdiensten sollten der vorliegenden Richtlinie unterliegen, wenn sie mindestens einen der Schritte in der Postzustellkette und insbesondere Abholung, Sortierung oder Zustellung, einschließlich Abholung durch den Empfänger, anbieten. ***Transport- und Lieferdienste***, die nicht in Verbindung mit einem dieser Schritte erbracht werden, sollten nicht unter Postdienste fallen.

[18] Richtlinie 97/67/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über gemeinsame Vorschriften für die Entwicklung des Binnenmarktes der Postdienste der Gemeinschaft und die Verbesserung der Dienstequalität (ABl. L 15 vom 21.1.1998, S. 14).

[18] Richtlinie 97/67/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über gemeinsame Vorschriften für die Entwicklung des Binnenmarktes der Postdienste der Gemeinschaft und die Verbesserung der Dienstequalität (ABl. L 15 vom 21.1.1998, S. 14).

Änderungsantrag 10

Vorschlag für eine Richtlinie
Erwägung 27 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(27a) Die Mitgliedstaaten sollten in ihren nationalen Cybersicherheitsstrategien auf die spezifischen Cybersicherheitsbedürfnisse von KMU eingehen, zu denen insbesondere ein schwach ausgeprägtes Cybersicherheitsbewusstsein, ungenügende IT-Sicherheit bei Remote-Anwendungen, hohe Kosten von Cybersicherheitslösungen und ein erhöhtes Bedrohungsniveau gehören. Die Mitgliedstaaten sollten über eine Anlaufstelle für Cybersicherheit für KMU verfügen, die einschlägige Informationen, Dienste und Orientierungshilfen bereitstellt.

Änderungsantrag 11

Vorschlag für eine Richtlinie
Erwägung 33

Vorschlag der Kommission	*Geänderter Text*
(33) Bei der Ausarbeitung von Leitfäden sollte die Kooperationsgruppe konsequent nationale Lösungen und Erfahrungen erfassen, die Auswirkungen ihrer Vorgaben auf nationale Ansätze bewerten, Herausforderungen bei der Umsetzung erörtern und spezifische Empfehlungen für eine bessere Umsetzung bestehender	(33) Bei der Ausarbeitung von Leitfäden sollte die Kooperationsgruppe konsequent nationale Lösungen und Erfahrungen erfassen, die Auswirkungen ihrer Vorgaben auf nationale Ansätze bewerten, Herausforderungen bei der Umsetzung erörtern und spezifische Empfehlungen – ***insbesondere mit Blick auf die Förderung***

Vorschriften formulieren.	***der Harmonisierung der Umsetzung dieser Richtlinie zwischen den Mitgliedstaaten –*** für eine bessere Umsetzung bestehender Vorschriften formulieren. ***Die Kooperationsgruppe sollte auch eine Bestandsaufnahme der nationalen Lösungen vornehmen, um die Kompatibilität von Cybersicherheitslösungen zu fördern, die für jeden einzelnen Sektor in ganz Europa angewandt werden. Dies gilt insbesondere für Sektoren mit internationalem und grenzüberschreitendem Charakter wie den Verkehrssektor.***

Änderungsantrag 12

Vorschlag für eine Richtlinie
Erwägung 34

Vorschlag der Kommission	*Geänderter Text*
(34) Die Kooperationsgruppe sollte ein flexibles Forum bleiben und in der Lage sein, unter Berücksichtigung der verfügbaren Ressourcen auf sich ändernde und neue politische Prioritäten und Herausforderungen zu reagieren. Sie sollte regelmäßige gemeinsame Sitzungen mit einschlägigen privaten Interessenträgern aus der gesamten Union organisieren, um die Tätigkeiten der Gruppe zu erörtern und Beiträge zu neuen politischen Herausforderungen einzuholen. Um die Zusammenarbeit auf Unionsebene zu verbessern, sollte die Gruppe in Erwägung ziehen, mit Cybersicherheitspolitik befasste Einrichtungen und Agenturen der Union, etwa das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3), die Agentur der Europäischen Union für Flugsicherheit (EASA) ***und*** die Agentur der Europäischen Union für das Weltraumprogramm (EUSPA), zur Teilnahme an ihrer Arbeit einzuladen.	(34) Die Kooperationsgruppe sollte ein flexibles Forum bleiben und in der Lage sein, unter Berücksichtigung der verfügbaren Ressourcen auf sich ändernde und neue politische Prioritäten und Herausforderungen zu reagieren. Sie sollte regelmäßige gemeinsame Sitzungen mit einschlägigen privaten Interessenträgern aus der gesamten Union organisieren, um die Tätigkeiten der Gruppe zu erörtern und Beiträge zu neuen politischen Herausforderungen einzuholen. Um die Zusammenarbeit auf Unionsebene zu verbessern, sollte die Gruppe in Erwägung ziehen, ***gegebenenfalls*** mit Cybersicherheitspolitik befasste Einrichtungen und Agenturen der Union, etwa das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3), ***das Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit, die für Verkehrssicherheit zuständigen Agenturen der Europäischen Union –*** die Agentur der Europäischen Union für Flugsicherheit (EASA)***, die Europäische***

	Agentur für die Sicherheit des Seeverkehrs (EMSA), die Eisenbahnagentur der Europäischen Union (ERA) –, die Agentur der Europäischen Union für das Weltraumprogramm (EUSPA) ***und alle anderen Einrichtungen und Agenturen, deren Fachwissen für die Debatten der Gruppe von Belang ist***, zur Teilnahme an ihrer Arbeit einzuladen.

Änderungsantrag 13

Vorschlag für eine Richtlinie
Erwägung 37 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(37a) Zu große Unterschiede bei der Umsetzung dieser Richtlinie durch die Mitgliedstaaten mit Blick auf das Risikomanagement und die Meldepflichten im Bereich Cybersicherheit könnten das gemeinsame Cybersicherheitsniveau in der Union gefährden. Die ENISA sollte deshalb in ihren Zweijahresberichten zum Stand der Cybersicherheit in der Union in Zusammenarbeit mit der Kommission abschätzen, inwieweit zwischen den Mitgliedstaaten Unterschiede beim Risikomanagement und bei den Meldepflichten im Bereich der Cybersicherheit bestehen.

Änderungsantrag 14

Vorschlag für eine Richtlinie
Erwägung 46 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(46a) Um kritische Lieferketten zu erhalten und zu schützen, sollte der Schwerpunkt auch auf dem Schutz der gesamten Transport- und Logistikkette liegen. Die Transport- und Logistikketten setzen sich aus zahlreichen miteinander

verbundenen Akteuren und Systemen zusammen, bei denen Güter intermodal in der Luft, auf der Straße, auf der Schiene, per Binnen- und per Seeverkehr befördert werden. Dieser Prozess erfordert einen raschen und zuverlässigen Datenaustausch zwischen den verschiedenen Gliedern der Transport- und Logistikkette über verschiedene Schnittstellen. Aufgrund der Verflechtung der verschiedenen Kettenglieder könnte eine unzureichende Cybersicherheit den störungsfreien Betrieb der gesamten Kette gefährden, wenn ein Cybersicherheitsvorfall in einem oder mehreren Teilen der Transport- und Logistikkette Dominoeffekte auslöst.

Änderungsantrag 15

Vorschlag für eine Richtlinie
Erwägung 47

Vorschlag der Kommission	*Geänderter Text*
(47) Bei den Lieferketten-Risikobewertungen unter Berücksichtigung der Besonderheiten des jeweiligen Sektors sollte sowohl technischen wie auch gegebenenfalls nichttechnischen Faktoren Rechnung getragen werden, einschließlich derer, die in der Empfehlung (EU) 2019/534, in der EU-weit koordinierten Risikobewertung zur Cybersicherheit in 5G-Netzen sowie in dem von der Kooperationsgruppe vereinbarten EU-Instrumentarium für die 5G-Cybersicherheit definiert sind. Bei der Ermittlung der Lieferketten, die einer koordinierten Risikobewertung unterzogen werden sollten, sollten folgende Kriterien berücksichtigt werden: i) der Umfang, in dem wesentliche und wichtige Einrichtungen bestimmte kritische IKT-Dienste, -Systeme oder -Produkte nutzen und auf sie angewiesen sind; ii) die Bedeutung bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte für die Ausführung kritischer oder sensibler	(47) Bei den Lieferketten-Risikobewertungen unter Berücksichtigung der Besonderheiten des jeweiligen Sektors sollte sowohl technischen wie auch gegebenenfalls nichttechnischen Faktoren Rechnung getragen werden, einschließlich derer, die in der Empfehlung (EU) 2019/534, in der EU-weit koordinierten Risikobewertung zur Cybersicherheit in 5G-Netzen sowie in dem von der Kooperationsgruppe vereinbarten EU-Instrumentarium für die 5G-Cybersicherheit definiert sind. Bei der Ermittlung der Lieferketten, die einer koordinierten Risikobewertung unterzogen werden sollten, sollten folgende Kriterien berücksichtigt werden: i) der Umfang, in dem wesentliche und wichtige Einrichtungen bestimmte kritische IKT-Dienste, -Systeme oder -Produkte nutzen und auf sie angewiesen sind; ii) die Bedeutung bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte für die Ausführung kritischer oder sensibler

Funktionen, einschließlich der Verarbeitung personenbezogener Daten; iii) die Verfügbarkeit alternativer IKT-Dienste, -Systeme oder -Produkte; iv) die Resilienz der gesamten Lieferkette von IKT-Diensten, -Systemen oder -Produkten gegen destabilisierende Ereignisse und v) die potenzielle künftige Bedeutung neuer IKT-Dienste, -Systeme oder -Produkte für die Tätigkeiten der Einrichtungen.	Funktionen, einschließlich der Verarbeitung personenbezogener Daten; iii) die Verfügbarkeit alternativer IKT-Dienste, -Systeme oder -Produkte; iv) die Resilienz der gesamten Lieferkette von IKT-Diensten, -Systemen oder -Produkten gegen destabilisierende Ereignisse***; (iva) das Maß, in dem bestimmte kritische IKT-Dienste, -Systeme oder -Produkte, die unmittelbar von Verbrauchern genutzt werden, widerstandsfähig sind und einem verbraucherfreundlichen Konzept entsprechen,*** und v) die potenzielle künftige Bedeutung neuer IKT-Dienste, -Systeme oder -Produkte für die Tätigkeiten der Einrichtungen.

Änderungsantrag 16

Vorschlag für eine Richtlinie
Erwägung 55

Vorschlag der Kommission	*Geänderter Text*
(55) Mit dieser Richtlinie wird ein zweistufiger Ansatz für die Meldung von Sicherheitsvorfällen festgelegt, um die richtige Balance herzustellen zwischen einer zeitnahen Meldung einerseits, die einer potenziellen Ausbreitung von Sicherheitsvorfällen entgegenwirkt und den Einrichtungen die Möglichkeit gibt, Unterstützung zu erhalten, und einer detaillierten Meldung andererseits, bei der aus individuellen Sicherheitsvorfällen wichtige Lehren gezogen werden und einzelne Unternehmen und ganze Sektoren ihre Resilienz gegenüber Cyberbedrohungen im Laufe der Zeit verbessern können. Erhalten Einrichtungen Kenntnis von einem Sicherheitsvorfall, sollten sie innerhalb von ***24*** Stunden eine erste Meldung übermitteln und spätestens einen Monat danach einen Abschlussbericht vorlegen müssen. Die Erstmeldung sollte nur die Informationen enthalten, die unbedingt erforderlich sind, um die zuständigen Behörden über den Sicherheitsvorfall zu unterrichten und es	(55) Mit dieser Richtlinie wird ein zweistufiger Ansatz für die Meldung von Sicherheitsvorfällen festgelegt, um die richtige Balance herzustellen zwischen einer zeitnahen Meldung einerseits, die einer potenziellen Ausbreitung von Sicherheitsvorfällen entgegenwirkt und den Einrichtungen die Möglichkeit gibt, Unterstützung zu erhalten, und einer detaillierten Meldung andererseits, bei der aus individuellen Sicherheitsvorfällen wichtige Lehren gezogen werden und einzelne Unternehmen und ganze Sektoren ihre Resilienz gegenüber Cyberbedrohungen im Laufe der Zeit verbessern können. Erhalten Einrichtungen Kenntnis von einem Sicherheitsvorfall, sollten sie innerhalb von ***36*** Stunden eine erste Meldung übermitteln und spätestens einen Monat danach einen Abschlussbericht vorlegen müssen. Die Erstmeldung sollte nur die Informationen enthalten, die unbedingt erforderlich sind, um die zuständigen Behörden über den Sicherheitsvorfall zu unterrichten und es

der Einrichtung zu ermöglichen, bei Bedarf Hilfe in Anspruch zu nehmen. Gegebenenfalls sollte aus dieser Meldung hervorgehen, ob der Sicherheitsvorfall vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist. Die Mitgliedstaaten sollten sicherstellen, dass durch die Pflicht zur Übermittlung dieser Erstmeldung die Ressourcen der meldenden Einrichtung für Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen, die Vorrang haben sollten, nicht beeinträchtigt werden. ***Zur weiteren Verhinderung***, dass die Meldepflichten für Sicherheitsvorfälle entweder zulasten der Ressourcen gehen, auf solche Vorfälle zu reagieren, oder entsprechende Anstrengungen der Einrichtungen anderweitig beeinträchtigt werden, sollten die Mitgliedstaaten auch vorsehen, dass die betreffende Einrichtung in hinreichend begründeten Fällen und im Einvernehmen mit den zuständigen Behörden oder dem CSIRT von der Frist von ***24*** Stunden für die Erstmeldung bzw. einem Monat für den Abschlussbericht abweichen kann.

der Einrichtung zu ermöglichen, bei Bedarf Hilfe in Anspruch zu nehmen. Gegebenenfalls sollte aus dieser Meldung hervorgehen, ob der Sicherheitsvorfall vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist. Die Mitgliedstaaten sollten sicherstellen, dass durch die Pflicht zur Übermittlung dieser Erstmeldung die Ressourcen der meldenden Einrichtung für Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen, die Vorrang haben sollten, nicht beeinträchtigt werden. ***Um weiter zu verhindern***, dass die Meldepflichten für Sicherheitsvorfälle entweder zulasten der Ressourcen gehen, auf solche Vorfälle zu reagieren, oder entsprechende Anstrengungen der Einrichtungen anderweitig beeinträchtigt werden, sollten die Mitgliedstaaten auch vorsehen, dass die betreffende Einrichtung in hinreichend begründeten Fällen und im Einvernehmen mit den zuständigen Behörden oder dem CSIRT von der Frist von ***36*** Stunden für die Erstmeldung bzw. einem Monat für den Abschlussbericht abweichen kann.

Änderungsantrag 17

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 2 – Unterabsatz 2

Vorschlag der Kommission	*Geänderter Text*
Die Mitgliedstaaten erstellen eine Liste der gemäß den Buchstaben b bis f ermittelten Einrichtungen und übermitteln sie der Kommission bis zum [***6*** Monate nach Ablauf der Umsetzungsfrist]. Danach überprüfen die Mitgliedstaaten die Liste regelmäßig und mindestens alle zwei Jahre und aktualisieren sie gegebenenfalls.	Die Mitgliedstaaten erstellen ***in enger Zusammenarbeit mit einschlägigen Branchenvertretern*** eine Liste der gemäß den Buchstaben b bis f ermittelten Einrichtungen und übermitteln sie der Kommission bis zum [***sechs*** Monate nach Ablauf der Umsetzungsfrist]. Danach überprüfen die Mitgliedstaaten die Liste regelmäßig und mindestens alle zwei Jahre und aktualisieren sie gegebenenfalls.

Änderungsantrag 18

Vorschlag für eine Richtlinie
Artikel 2 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
(6) Wenn wesentliche oder wichtige Einrichtungen gemäß den Bestimmungen sektorspezifischer Rechtsakte der Union entweder Maßnahmen zum Cybersicherheitsrisikomanagement ergreifen oder Sicherheitsvorfälle und erhebliche Cyberbedrohungen melden müssen und wenn die entsprechenden Anforderungen in ihrer Wirkung den in dieser Richtlinie festgelegten Verpflichtungen, ***auch*** den in Kapitel VI festgelegten Bestimmungen in Bezug auf die Aufsicht und die Durchsetzung**,** zumindest gleichwertig sind, finden die einschlägigen Bestimmungen dieser Richtlinie keine Anwendung.	(6) Wenn wesentliche oder wichtige Einrichtungen gemäß den Bestimmungen sektorspezifischer Rechtsakte der Union entweder Maßnahmen zum Cybersicherheitsrisikomanagement ergreifen oder Sicherheitsvorfälle und erhebliche Cyberbedrohungen melden müssen und wenn die entsprechenden Anforderungen in ihrer Wirkung den in dieser Richtlinie festgelegten Verpflichtungen ***– auch in Bezug auf die Befugnisse***, ***das Mandat und die Funktionen der jeweiligen Aufsichtsbehörden – sowie*** den in Kapitel VI festgelegten Bestimmungen in Bezug auf die Aufsicht und die Durchsetzung zumindest gleichwertig sind, finden die einschlägigen Bestimmungen dieser Richtlinie keine Anwendung.

Änderungsantrag 19

Vorschlag für eine Richtlinie
Artikel 5 – Absatz 2 – Buchstabe h

Vorschlag der Kommission	*Geänderter Text*
h) ein Konzept, das auf die spezifischen Bedürfnisse von KMU – insbesondere vom Anwendungsbereich dieser Richtlinie ausgenommener KMU – ausgerichtet ist und Orientierungshilfen sowie Unterstützung bei der Verbesserung ihrer Resilienz gegenüber Cybersicherheitsbedrohungen bietet.	h) ein Konzept, das auf die spezifischen Bedürfnisse von KMU – insbesondere vom Anwendungsbereich dieser Richtlinie ausgenommener KMU – ausgerichtet ist und Orientierungshilfen***, die erforderlichen und umfassenden Informationen*** sowie Unterstützung bei der Verbesserung ihrer Resilienz gegenüber Cybersicherheitsbedrohungen bietet.

Änderungsantrag 20

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 4 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) Bereitstellung von Orientierungshilfen für die zuständigen Behörden in Bezug auf die Umsetzung und Durchführung dieser Richtlinie;	a) Bereitstellung von Orientierungshilfen für die zuständigen Behörden in Bezug auf die Umsetzung und Durchführung dieser Richtlinie***, um Unterschiede zwischen den Mitgliedstaaten bei den Standards des Risikomanagements und der Meldepflichten im Bereich der Cybersicherheit auf ein Mindestmaß zu verringern***;

Änderungsantrag 21

Vorschlag für eine Richtlinie
Artikel 12 – Absatz 4 – Buchstabe b a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ba) Vornahme einer Bestandsaufnahme der nationalen Lösungen, um die Kompatibilität von Cybersicherheitslösungen zu fördern, die für die einzelnen spezifischen Branchen in der gesamten Union angewendet werden;

Änderungsantrag 22

Vorschlag für eine Richtlinie
Artikel 15 – Absatz 1 – Buchstabe c a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ca) den Umfang der Unterschiede zwischen den Mitgliedstaaten beim Risikomanagement und bei den Meldepflichten im Bereich der Cybersicherheit und das Ausmaß, in dem sich diese Unterschiede auf das gemeinsame Cybersicherheitsniveau in der Union auswirken.

Änderungsantrag 23

Vorschlag für eine Richtlinie
Artikel 16 – Absatz 1 – Buchstabe iii a (neu)

Vorschlag der Kommission	*Geänderter Text*
	iiia) Empfehlungen zur Verbesserung der Kohärenz und der Rechtssicherheit bei der Auslegung und Anwendung dieser Richtlinie und der anwendbaren sektorspezifischen Rechtsvorschriften mit Schwerpunkt auf der Ermittlung und Beseitigung von Überschneidungen und Redundanzen in den jeweiligen Rechtsvorschriften, rechtlichen Anforderungen oder Verfahren;

Änderungsantrag 24

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 2 – Buchstabe b a (neu)

Vorschlag der Kommission	*Geänderter Text*
	ba) Strategien, Programme und Verfahren, um sicherzustellen, dass die Mitarbeiter über angemessene Kenntnisse, um Cybersicherheitsrisiken erkennen zu können, und über praktische Erfahrung in der Einhaltung hoher Cybersicherheitsstandards verfügen;

Änderungsantrag 25

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 2 – Buchstabe e

Vorschlag der Kommission	*Geänderter Text*
e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;	e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich ***mobiler Elemente wie Fahrzeuge und Fernsensoren, sowie*** Management und Offenlegung von Schwachstellen;

Änderungsantrag 26

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
(5) Die Kommission kann ***Durchführungsrechtsakte*** erlassen, um die technischen und methodischen Spezifikationen für die in Absatz 2 genannten Elemente festzulegen. ***Bei der Ausarbeitung dieser Rechtsakte verfährt*** die ***Kommission nach dem Prüfverfahren*** gemäß Artikel ***37 Absatz 2*** und ***beachtet dabei*** so weit wie möglich ***internationale*** und ***europäische*** Normen sowie ***die*** einschlägigen technischen Spezifikationen.	(5) Die Kommission kann ***delegierte Rechtsakte*** erlassen, um die technischen und methodischen Spezifikationen für die in Absatz 2 genannten Elemente festzulegen. Die ***delegierten Rechtsakte werden*** gemäß Artikel ***36 erlassen*** und ***folgen*** so weit wie möglich ***internationalen*** und ***europäischen*** Normen sowie einschlägigen technischen Spezifikationen.

Änderungsantrag 27

Vorschlag für eine Richtlinie
Artikel 18 – Absatz 6 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(6a) Im Interesse einer wirksamen Politik und ihrer einfacheren Umsetzung konsultiert die Kommission insbesondere vor dem Erlass der delegierten Rechtakte gemäß den Absätzen 5 und 6 wesentliche und wichtige Einrichtungen.

Änderungsantrag 28

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Unterabsatz 1 – Buchstabe a

Vorschlag der Kommission	*Geänderter Text*
a) unverzüglich, in jedem Fall aber innerhalb von ***24*** Stunden nach Kenntnisnahme des Sicherheitsvorfalls, eine erste Meldung, in der gegebenenfalls angegeben wird, ob der Sicherheitsvorfall vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist;	a) unverzüglich, in jedem Fall aber innerhalb von ***36*** Stunden nach Kenntnisnahme des Sicherheitsvorfalls, eine erste Meldung, in der gegebenenfalls angegeben wird, ob der Sicherheitsvorfall vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist;

Änderungsantrag 29

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 4 – Unterabsatz 1 – Buchstabe c – Ziffer iii

Vorschlag der Kommission	*Geänderter Text*
iii) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen.	iii) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen ***sowie zu deren Ergebnissen***.

Änderungsantrag 30

Vorschlag für eine Richtlinie
Artikel 20 – Absatz 11

Vorschlag der Kommission	*Geänderter Text*
(11) Die Kommission kann ***Durchführungsrechtsakte*** erlassen, in denen die Art der Angaben, das Format und das Verfahren für Meldungen gemäß den Absätzen 1 und 2 näher bestimmt werden. Die Kommission kann ferner Durchführungsrechtsakte erlassen, um genauer zu bestimmen, in welchen Fällen ein Sicherheitsvorfall als erheblich im Sinne des Absatzes 3 anzusehen ist. Diese Durchführungsrechtsakte werden ***nach*** dem in Artikel 37 Absatz 2 genannten Prüfverfahren erlassen.	(11) Die Kommission kann ***delegierte Rechtsakte gemäß Artikel 36*** erlassen, in denen die Art der Angaben, das Format und das Verfahren für Meldungen gemäß den Absätzen 1 und 2 ***dieses Artikels*** näher bestimmt werden. Die Kommission kann ferner Durchführungsrechtsakte erlassen, um genauer zu bestimmen, in welchen Fällen ein Sicherheitsvorfall als erheblich im Sinne des Absatzes 3 anzusehen ist. Diese Durchführungsrechtsakte werden ***gemäß*** dem in Artikel 37 Absatz 2 genannten Prüfverfahren erlassen.

Änderungsantrag 31

Vorschlag für eine Richtlinie
Artikel 21 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
(1) Die Mitgliedstaaten ***können*** wesentliche und wichtige Einrichtungen ***dazu verpflichten***, bestimmte IKT-Produkte, -Dienste und -Prozesse im Rahmen spezifischer europäischer Systeme für die Cybersicherheitszertifizierung, die gemäß Artikel 49 der Verordnung (EU) 2019/881 angenommen wurden, zertifizieren zu lassen, um die Erfüllung	(1) Die Mitgliedstaaten ***bestärken*** wesentliche und wichtige Einrichtungen ***darin***, bestimmte IKT-Produkte, -Dienste und -Prozesse***, die entweder von der wesentlichen oder wichtigen Einrichtung entwickelt oder von Dritten beschafft wurden,*** im Rahmen spezifischer europäischer Systeme für die Cybersicherheitszertifizierung, die gemäß

bestimmter in Artikel 18 genannter Anforderungen nachzuweisen. ***Die zu zertifizierenden Produkte, Dienstleistungen und Prozesse können von einer wesentlichen oder wichtigen Einrichtung entwickelt oder von Dritten beschafft worden sein.***	Artikel 49 der Verordnung (EU) 2019/881 angenommen wurden, ***oder im Rahmen ähnlicher international anerkannter Zertifizierungssysteme*** zertifizieren zu lassen, um die Erfüllung bestimmter in Artikel 18 genannter Anforderungen nachzuweisen.

Änderungsantrag 32

Vorschlag für eine Richtlinie
Artikel 21 – Absatz 1 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(1a) Die in dieser Richtlinie enthaltenen Anforderungen an die Cybersicherheitszertifizierung lassen Artikel 56 Absätze 2 und 3 der Verordnung (EU) 2019/881 unberührt.

Änderungsantrag 33

Vorschlag für eine Richtlinie
Artikel 21 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
(2) Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte zu erlassen, in denen ausgeführt wird, welche Kategorien wesentlicher Einrichtungen ein Zertifikat erlangen müssen und welche spezifischen europäischen Systeme für die Cybersicherheitszertifizierung dabei nach Absatz 1 anzuwenden sind. Die delegierten Rechtsakte werden gemäß Artikel 36 erlassen.	***entfällt***

Änderungsantrag 34

Vorschlag für eine Richtlinie
Artikel 21 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
(3) ***Ist kein geeignetes europäisches***	(3) ***Um die Abwehrfähigkeit im***

System für die Cybersicherheitszertifizierung für die Zwecke des Absatzes 2 vorhanden, kann die Kommission die ENISA auffordern, ein vorläufiges System gemäß ***Artikel*** 48 ***Absatz 2*** der Verordnung (EU) 2019/881 auszuarbeiten.	***Bereich der Cybersicherheit insgesamt zu erhöhen***, kann die Kommission die ENISA auffordern, ein vorläufiges System gemäß ***den Artikeln 47 und*** 48 der Verordnung (EU) 2019/881 auszuarbeiten***, wenn kein geeignetes europäisches System für die Cybersicherheitszertifizierung verfügbar ist. Ein solches vorläufiges System muss die in Artikel 56 Absätze 2 und 3 der Verordnung (EU) 2019/881 genannten Anforderungen erfüllen.***

VERFAHREN DES MITBERATENDEN AUSSCHUSSES

Titel	Maßnahmen zur Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus in der Union, Aufhebung der Richtlinie (EU) 2016/1148
Bezugsdokumente – Verfahrensnummer	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Federführender Ausschuss Datum der Bekanntgabe im Plenum	ITRE 21.1.2021
Stellungnahme von Datum der Bekanntgabe im Plenum	TRAN 21.1.2021
Verfasser(in) der Stellungnahme Datum der Benennung	Jakop G. Dalunde 3.2.2021
Datum der Annahme	12.7.2021
Ergebnis der Schlussabstimmung	+: 48 –: 0 0: 1
Zum Zeitpunkt der Schlussabstimmung anwesende Mitglieder	Magdalena Adamowicz, Andris Ameriks, Izaskun Bilbao Barandica, Paolo Borchia, Marco Campomenosi, Massimo Casanova, Ciarán Cuffe, Jakop G. Dalunde, Johan Danielsson, Karima Delli, Anna Deparnay-Grunenberg, Gheorghe Falcă, Giuseppe Ferrandino, Mario Furore, Søren Gade, Isabel García Muñoz, Elsi Katainen, Kateřina Konečná, Julie Lechanteux, Peter Lundgren, Benoît Lutgen, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Tilly Metz, Cláudia Monteiro de Aguiar, Caroline Nagtegaal, Jan-Christoph Oetjen, Philippe Olivier, João Pimenta Lopes, Rovana Plumb, Dominique Riquet, Dorien Rookmaker, Massimiliano Salini, Sven Schulze, Vera Tax, Barbara Thaler, Henna Virkkunen, Petar Vitanov, Elissavet Vozemberg-Vrionidi, Roberts Zīle, Kosma Złotowski
Zum Zeitpunkt der Schlussabstimmung anwesende Stellvertreter	Clare Daly, Nicola Danti, Angel Dzhambazki, Tomasz Frankowski, Michael Gahler, Maria Grapini, Alessandra Moretti, Marianne Vind

NAMENTLICHE SCHLUSSABSTIMMUNG IM MITBERATENDEN AUSSCHUSS

48	+
ECR	Angel Dzhambazki, Peter Lundgren, Roberts Zīle, Kosma Złotowski
ID	Paolo Borchia, Marco Campomenosi, Massimo Casanova, Julie Lechanteux, Philippe Olivier
NI	Mario Furore, Dorien Rookmaker
PPE	Magdalena Adamowicz, Gheorghe Falcă, Tomasz Frankowski, Michael Gahler, Elżbieta Katarzyna Łukacijewska, Benoît Lutgen, Marian-Jean Marinescu, Cláudia Monteiro de Aguiar, Massimiliano Salini, Sven Schulze, Barbara Thaler, Henna Virkkunen, Elissavet Vozemberg-Vrionidi
Renew	Izaskun Bilbao Barandica, Nicola Danti, Søren Gade, Elsi Katainen, Caroline Nagtegaal, Jan-Christoph Oetjen, Dominique Riquet
S&D	Andris Ameriks, Johan Danielsson, Giuseppe Ferrandino, Isabel García Muñoz, Maria Grapini, Alessandra Moretti, Rovana Plumb, Vera Tax, Marianne Vind, Petar Vitanov
The Left	Clare Daly, Kateřina Konečná
Verts/ALE	Ciarán Cuffe, Jakop G. Dalunde, Karima Delli, Anna Deparnay-Grunenberg, Tilly Metz

0	-

1	0
The Left	João Pimenta Lopes

Erklärung der benutzten Zeichen:
+ : dafür
- : dagegen
0 : Enthaltung

VERFAHREN DES FEDERFÜHRENDEN AUSSCHUSSES

Titel	Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und Aufhebung der Richtlinie (EU) 2016/1148			
Bezugsdokumente – Verfahrensnummer	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)			
Datum der Übermittlung an das EP	16.12.2020			
Federführender Ausschuss Datum der Bekanntgabe im Plenum	ITRE 21.1.2021			
Mitberatende Ausschüsse Datum der Bekanntgabe im Plenum	AFET 21.1.2021	ECON 21.1.2021	IMCO 21.1.2021	TRAN 21.1.2021
	CULT 21.1.2021	LIBE 21.1.2021		
Nicht abgegebene Stellungnahme(n) Datum des Beschlusses	ECON 26.1.2021	CULT 11.1.2021		
Assoziierte Ausschüsse Datum der Bekanntgabe im Plenum	LIBE 20.5.2021			
Berichterstatter(in/innen) Datum der Benennung	Bart Groothuis 14.1.2021			
Prüfung im Ausschuss	13.4.2021	26.5.2021		
Datum der Annahme	28.10.2021			
Ergebnis der Schlussabstimmung	+: –: 0:	70 3 1		
Zum Zeitpunkt der Schlussabstimmung anwesende Mitglieder	Nicola Beer, François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Vasile Blaga, Michael Bloss, Manuel Bompard, Paolo Borchia, Marc Botenga, Markus Buchheit, Cristian-Silviu Buşoi, Carlo Calenda, Maria da Graça Carvalho, Ignazio Corrao, Ciarán Cuffe, Josianne Cutajar, Nicola Danti, Pilar del Castillo Vera, Christian Ehler, Valter Flego, Niels Fuglsang, Lina Gálvez Muñoz, Claudia Gamon, Bart Groothuis, Christophe Grudler, András Gyürk, Henrike Hahn, Robert Hajšel, Ivo Hristov, Ivars Ijabs, Romana Jerković, Eva Kaili, Seán Kelly, Izabela-Helena Kloc, Łukasz Kohut, Zdzisław Krasnodębski, Andrius Kubilius, Miapetra Kumpula-Natri, Thierry Mariani, Marisa Matias, Eva Maydell, Georg Mayer, Joëlle Mélin, Dan Nica, Angelika Niebler, Ville Niinistö, Aldo Patriciello, Mauri Pekkarinen, Tsvetelina Penkova, Morten Petersen, Markus Pieper, Clara Ponsatí Obiols, Manuela Ripa, Robert Roos, Sara Skyttedal, Maria Spyraki, Jessica Stegrud, Beata Szydło, Riho Terras, Grzegorz Tobiszowski, Isabella Tovaglieri, Viktor Uspaskich, Henna Virkkunen, Pernille Weiss, Carlos Zorrinho			
Zum Zeitpunkt der Schlussabstimmung anwesende Stellvertreter	Rasmus Andresen, Marek Paweł Balt, Klemen Grošelj, Adam Jarubas, Elena Lizzi, Adriana Maldonado López, Bronis Ropė, Jordi Solé, Nils Torvalds			
Datum der Einreichung	4.11.2021			

NAMENTLICHE SCHLUSSABSTIMMUNG IM FEDERFÜHRENDEN AUSSCHUSS

70	+
ECR	Izabela-Helena Kloc, Zdzisław Krasnodębski, Robert Roos, Beata Szydło, Grzegorz Tobiszowski
ID	Paolo Borchia, Markus Buchheit, Elena Lizzi, Thierry Mariani, Georg Mayer, Joëlle Mélin, Isabella Tovaglieri
NI	András Gyürk, Clara Ponsatí Obiols, Viktor Uspaskich
PPE	François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Vasile Blaga, Cristian-Silviu Buşoi, Maria da Graça Carvalho, Pilar del Castillo Vera, Christian Ehler, Adam Jarubas, Seán Kelly, Andrius Kubilius, Eva Maydell, Angelika Niebler, Aldo Patriciello, Markus Pieper, Sara Skyttedal, Maria Spyraki, Riho Terras, Henna Virkkunen, Pernille Weiss
Renew	Nicola Beer, Nicola Danti, Valter Flego, Claudia Gamon, Bart Groothuis, Klemen Grošelj, Christophe Grudler, Ivars Ijabs, Mauri Pekkarinen, Morten Petersen, Nils Torvalds
S&D	Marek Paweł Balt, Carlo Calenda, Josianne Cutajar, Niels Fuglsang, Lina Gálvez Muñoz, Robert Hajšel, Ivo Hristov, Romana Jerković, Eva Kaili, Łukasz Kohut, Miapetra Kumpula-Natri, Adriana Maldonado López, Dan Nica, Tsvetelina Penkova, Carlos Zorrinho
Verts/ALE	Rasmus Andresen, Michael Bloss, Ignazio Corrao, Ciarán Cuffe, Henrike Hahn, Ville Niinistö, Manuela Ripa, Bronis Ropė, Jordi Solé

3	-
The Left	Manuel Bompard, Marc Botenga, Marisa Matias

1	0
ECR	Jessica Stegrud

Erklärung der benutzten Zeichen:
+ : dafür
- : dagegen
0 : Enthaltung