



2017/0225(COD)

2.3.2018

ÄNDERUNGSANTRÄGE

52 – 366

Entwurf einer Stellungnahme

Nicola Danti

(PE616.831v01-00)

Verordnung über die „EU-Cybersicherheitsagentur“ (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit“)

Vorschlag für eine Verordnung

(COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

Änderungsantrag 52
Jan Philipp Albrecht

Vorschlag für eine Verordnung
Titel

Vorschlag der Kommission

Vorschlag für eine
VERORDNUNG DES EUROPÄISCHEN
PARLAMENTS UND DES RATES
über die „**EU-Cybersicherheitsagentur**“
(ENISA) und zur Aufhebung der
Verordnung (EU) Nr. 526/2013 sowie über
die Zertifizierung der **Cybersicherheit** von
Informations- und Kommunikationstechnik
(„Rechtsakt zur **Cybersicherheit**“)

(Text von Bedeutung für den EWR)

Geänderter Text

Vorschlag für eine
VERORDNUNG DES EUROPÄISCHEN
PARLAMENTS UND DES RATES
über die „**Agentur der Europäischen
Union für Netz- und
Informationssicherheit**“ (ENISA) und zur
Aufhebung der Verordnung (EU)
Nr. 526/2013 sowie über die Zertifizierung
der **IT-Sicherheit** von Informations- und
Kommunikationstechnik („Rechtsakt zur
IT-Sicherheit“)

(Text von Bedeutung für den EWR)

*(Dieser Änderungsantrag betrifft den
gesamten Text. Seine Annahme würde
entsprechende Abänderungen im gesamten
Text erforderlich machen.)*

Or. en

Begründung

Das Präfix „Cyber“ leitet sich von der Science-Fiction-Literatur der 1960er ab und wird immer mehr zur Beschreibung der negativen Aspekte des Internets („Cyberangriff“, „Cyberkriminalität“) verwendet, ist rechtlich aber äußerst unscharf. Im Sinne der Rechtssicherheit wird daher vorgeschlagen, den Begriff „Cybersicherheit“ durch den Begriff „IT-Sicherheit“ zu ersetzen.

Änderungsantrag 53
Jiří Pospíšil

Vorschlag für eine Verordnung
Erwägung 1

Vorschlag der Kommission

(1) Netz- und Informationssysteme
sowie Telekommunikationsnetze und -
dienste spielen eine lebenswichtige Rolle

Geänderter Text

(1) Netz- und Informationssysteme
sowie Telekommunikationsnetze und -
dienste spielen eine lebenswichtige Rolle

für die Gesellschaft und sind mittlerweile zum Hauptmotor des Wirtschaftswachstums geworden. Die Informations- und Kommunikationstechnik **bildet das Rückgrat der komplexen** Systeme, die gesellschaftliche Tätigkeiten unterstützen und unsere Volkswirtschaften in Schlüsselsektoren wie Gesundheit, Energie, Finanzen und Verkehr aufrechterhalten und die insbesondere dafür sorgen, dass der Binnenmarkt reibungslos funktioniert.

für die Gesellschaft und sind mittlerweile zum Hauptmotor des Wirtschaftswachstums geworden. Die Informations- und Kommunikationstechnik **(nachstehend IKT) stellt komplexe** Systeme dar, die **übliche** gesellschaftliche Tätigkeiten unterstützen und unsere Volkswirtschaften in Schlüsselsektoren wie Gesundheit, Energie, Finanzen und Verkehr aufrechterhalten und die insbesondere dafür sorgen, dass der Binnenmarkt reibungslos funktioniert.

Or. cs

Änderungsantrag 54 **Philippe Juvin**

Vorschlag für eine Verordnung **Erwägung 2**

Vorschlag der Kommission

(2) Die Nutzung von Netz- und Informationssystemen durch Bürger, Unternehmen und Behörden ist mittlerweile in der Union allgegenwärtig. Digitalisierung und Konnektivität entwickeln sich zu Kernmerkmalen einer ständig steigenden Zahl von Produkten und Dienstleistungen. Mit dem Aufkommen des Internets der Dinge dürften in den nächsten Jahrzehnten Millionen, wenn nicht Milliarden vernetzte digitale Geräte unionsweit Verbreitung finden. Zwar sind immer mehr Geräte mit dem Internet vernetzt, doch verfügen sie über eine nur unzureichende Cybersicherheit, da die Sicherheit und Abwehrfähigkeit dieser Geräte schon bei der Konzeption nicht ausreichend berücksichtigt wurden. Vor diesem Hintergrund führt die geringe Zertifizierung dazu, dass Personen, die IKT-Produkte und -Dienste für unternehmerische oder private Zwecke nutzen, nur unzureichend über deren Cybersicherheitsmerkmale informiert

Geänderter Text

(2) Die Nutzung von Netz- und Informationssystemen durch Bürger, Unternehmen und Behörden ist mittlerweile in der Union allgegenwärtig. Digitalisierung und Konnektivität entwickeln sich zu Kernmerkmalen einer ständig steigenden Zahl von Produkten und Dienstleistungen. Mit dem Aufkommen des Internets der Dinge dürften in den nächsten Jahrzehnten Millionen, wenn nicht Milliarden vernetzte digitale Geräte unionsweit Verbreitung finden. Zwar sind immer mehr Geräte mit dem Internet vernetzt, doch verfügen sie über eine nur unzureichende Cybersicherheit, da die Sicherheit und Abwehrfähigkeit dieser Geräte schon bei der Konzeption nicht ausreichend berücksichtigt wurden. Vor diesem Hintergrund führt die geringe Zertifizierung dazu, dass Personen, die IKT-Produkte und -Dienste für unternehmerische oder private Zwecke nutzen, nur unzureichend über deren Cybersicherheitsmerkmale informiert

werden, wodurch das Vertrauen in digitale Lösungen untergraben wird.

werden, wodurch das Vertrauen in digitale Lösungen untergraben wird, **das für die Schaffung des digitalen Binnenmarkts essentiell ist.**

Or. fr

Änderungsantrag 55

Liisa Jaakonsaari, Christel Schaldemose, Lucy Anderson

Vorschlag für eine Verordnung

Erwägung 3

Vorschlag der Kommission

(3) Mit der zunehmenden Digitalisierung und Vernetzung steigen auch die Cybersicherheitsrisiken, wodurch die Gesellschaft insgesamt anfälliger für Cyberbedrohungen wird und die Gefahren zunehmen, denen Privatpersonen und insbesondere schutzbedürftige Personengruppen wie Kinder ausgesetzt sind. Um **dieser Gefahr** für die Gesellschaft zu begegnen, gilt es alle für die Erhöhung der Cybersicherheit in der EU notwendigen Maßnahmen zu ergreifen, um die Netz- und Informationssysteme, die Telekommunikationsnetze und die digitalen Produkte, Dienste und Geräte, die von Privatpersonen, Behörden und Unternehmen – von KMU bis zu Betreibern kritischer Infrastrukturen – genutzt werden, vor Cyberbedrohungen zu schützen.

Geänderter Text

(3) Mit der zunehmenden Digitalisierung und Vernetzung steigen auch die Cybersicherheitsrisiken, wodurch die Gesellschaft insgesamt anfälliger für Cyberbedrohungen wird und die Gefahren zunehmen, denen Privatpersonen und insbesondere schutzbedürftige Personengruppen wie Kinder ausgesetzt sind. **Die Veränderungskraft künstlicher Intelligenz und maschinellen Lernens wird von der Gesellschaft als Ganzes, aber auch von Cyberkriminellen genutzt werden.** Um **diesen Gefahren** für die Gesellschaft zu begegnen, gilt es alle für die Erhöhung der Cybersicherheit in der EU notwendigen Maßnahmen zu ergreifen, um die Netz- und Informationssysteme, die Telekommunikationsnetze und die digitalen Produkte, Dienste und Geräte, die von Privatpersonen, Behörden und Unternehmen – von KMU bis zu Betreibern kritischer Infrastrukturen – genutzt werden, vor Cyberbedrohungen zu schützen.

Or. en

Änderungsantrag 56

Maria Grapini

Vorschlag für eine Verordnung

Erwägung 3

Vorschlag der Kommission

(3) Mit der zunehmenden Digitalisierung und Vernetzung steigen auch die Cybersicherheitsrisiken, wodurch die Gesellschaft insgesamt anfälliger für Cyberbedrohungen wird und die Gefahren zunehmen, denen Privatpersonen und insbesondere schutzbedürftige Personengruppen wie Kinder ausgesetzt sind. Um dieser Gefahr für die Gesellschaft zu begegnen, gilt es alle für die Erhöhung der Cybersicherheit in der EU notwendigen Maßnahmen zu ergreifen, um die Netz- und Informationssysteme, die Telekommunikationsnetze und die digitalen Produkte, Dienste und Geräte, die von Privatpersonen, Behörden und Unternehmen – von KMU bis zu Betreibern kritischer Infrastrukturen – genutzt werden, vor Cyberbedrohungen zu schützen.

Geänderter Text

(3) Mit der zunehmenden Digitalisierung und Vernetzung steigen auch die Cybersicherheitsrisiken, wodurch die Gesellschaft insgesamt anfälliger für Cyberbedrohungen wird und die Gefahren zunehmen, denen Privatpersonen und insbesondere schutzbedürftige Personengruppen wie Kinder ausgesetzt sind. Um dieser Gefahr für die Gesellschaft zu begegnen, gilt es alle für die Erhöhung der Cybersicherheit **gegen Cyberangriffe** in der EU notwendigen Maßnahmen zu ergreifen, um die Netz- und Informationssysteme, die Telekommunikationsnetze und die digitalen Produkte, Dienste und Geräte, die von Privatpersonen, Behörden und Unternehmen – von KMU bis zu Betreibern kritischer Infrastrukturen – genutzt werden, vor Cyberbedrohungen zu schützen.

Or. ro

Änderungsantrag 57
Philippe Juvin

Vorschlag für eine Verordnung
Erwägung 3

Vorschlag der Kommission

(3) Mit der zunehmenden Digitalisierung und Vernetzung steigen auch die Cybersicherheitsrisiken, wodurch die Gesellschaft insgesamt anfälliger für Cyberbedrohungen wird und die Gefahren zunehmen, denen Privatpersonen und insbesondere schutzbedürftige Personengruppen wie Kinder ausgesetzt sind. Um dieser Gefahr für die Gesellschaft zu begegnen, gilt es alle für die Erhöhung der Cybersicherheit in der EU notwendigen Maßnahmen zu ergreifen, um die Netz-

Geänderter Text

(3) Mit der zunehmenden Digitalisierung und Vernetzung steigen auch die Cybersicherheitsrisiken **deutlich**, wodurch die Gesellschaft insgesamt anfälliger für Cyberbedrohungen wird und die Gefahren zunehmen, denen Privatpersonen und insbesondere schutzbedürftige Personengruppen wie Kinder ausgesetzt sind. Um dieser Gefahr für die Gesellschaft zu begegnen, gilt es alle für die Erhöhung der Cybersicherheit in der EU notwendigen Maßnahmen zu

und Informationssysteme, die Telekommunikationsnetze und die digitalen Produkte, Dienste und Geräte, die von Privatpersonen, Behörden und Unternehmen – von KMU bis zu Betreibern kritischer Infrastrukturen – genutzt werden, vor Cyberbedrohungen zu schützen.

ergreifen, um die Netz- und Informationssysteme, die Telekommunikationsnetze und die digitalen Produkte, Dienste und Geräte, die von Privatpersonen, Behörden und Unternehmen – von KMU bis zu Betreibern kritischer Infrastrukturen – genutzt werden, vor Cyberbedrohungen zu schützen.

Or. fr

Änderungsantrag 58

Maria Grapini

Vorschlag für eine Verordnung

Erwägung 4

Vorschlag der Kommission

(4) Cyberangriffe nehmen zu und eine Wirtschaft und Gesellschaft, die durch ihre Vernetzung anfälliger für Cyberbedrohungen und -angriffe ist, benötigt daher einen stärkeren Schutz. Auf die häufig grenzüberschreitenden Cyberangriffe reagieren die für die Cybersicherheit zuständigen Behörden jedoch vor allem mit nationalen Strategien, zumal die Zuständigkeiten für die Strafverfolgung an den nationalen Grenzen enden. Cybersicherheitsvorfälle großen Ausmaßes könnten die Bereitstellung wesentlicher Dienste in der gesamten EU empfindlich stören. Vonnöten sind daher effektive Maßnahmen und ein Krisenmanagement auf EU-Ebene, gestützt auf gezielte Strategien, sowie ein breiter angelegtes Instrumentarium für eine europäische Solidarität und gegenseitige Hilfe. Zudem sind eine auf zuverlässigen Daten der Union basierende regelmäßige Überprüfung des Stands der Cybersicherheit und Abwehrfähigkeit in der Union sowie eine systematische Prognose künftiger Entwicklungen, Herausforderungen und Bedrohungen –

Geänderter Text

(4) Cyberangriffe nehmen zu und eine Wirtschaft und Gesellschaft, die durch ihre Vernetzung anfälliger für Cyberbedrohungen und -angriffe ist, benötigt daher einen stärkeren **und sichereren** Schutz. Auf die häufig grenzüberschreitenden Cyberangriffe reagieren die für die Cybersicherheit zuständigen Behörden jedoch vor allem mit nationalen Strategien, zumal die Zuständigkeiten für die Strafverfolgung an den nationalen Grenzen enden. Cybersicherheitsvorfälle großen Ausmaßes könnten die Bereitstellung wesentlicher Dienste in der gesamten EU empfindlich stören. Vonnöten sind daher effektive Maßnahmen und ein Krisenmanagement auf EU-Ebene, gestützt auf gezielte Strategien, sowie ein breiter angelegtes Instrumentarium für eine europäische Solidarität und gegenseitige Hilfe. Zudem sind eine auf zuverlässigen Daten der Union basierende regelmäßige Überprüfung des Stands der Cybersicherheit und Abwehrfähigkeit in der Union sowie eine systematische Prognose künftiger Entwicklungen,

sowohl auf Unionsebene als auch auf globaler Ebene – für die Entscheidungsträger, die Branche und die Nutzer daher gleichermaßen wichtig.

Herausforderungen und Bedrohungen – sowohl auf Unionsebene als auch auf globaler Ebene – für die Entscheidungsträger, die Branche und die Nutzer daher gleichermaßen wichtig.

Or. ro

Änderungsantrag 59
Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Erwägung 5

Vorschlag der Kommission

(5) Angesichts immer größerer Herausforderungen, die sich der Union im Bereich der Cybersicherheit stellen, bedarf es eines umfassenden Maßnahmenpakets, das auf den bisherigen Maßnahmen der Union aufbaut und sich wechselseitig verstärkende Ziele unterstützt. Dies beinhaltet eine weitere Stärkung der Fähigkeiten und der Abwehrbereitschaft der Mitgliedstaaten und Unternehmen sowie eine bessere Zusammenarbeit und Koordinierung zwischen den Mitgliedstaaten und den Organen, Einrichtungen und Stellen der EU. Da Cyberbedrohungen an keinen Grenzen Halt machen, gilt es zudem, die Fähigkeiten auf Unionsebene zu stärken, die einzelstaatliche Maßnahmen vor allem dann ergänzen könnten, wenn es sich um grenzüberschreitende Cybersicherheitsvorfälle und -krisen von großem Ausmaß handelt. Darüber hinaus sind weitere Anstrengungen notwendig, um die Bürgerinnen und Bürger sowie die Unternehmen für Fragen der Cybersicherheit zu sensibilisieren. Ferner ließe sich das Vertrauen in den digitalen Binnenmarkt weiter erhöhen, wenn transparente Informationen über das Niveau der Sicherheit von IKT-Produkten und -Diensten zur Verfügung stünden.

Geänderter Text

(5) Angesichts immer größerer Herausforderungen, die sich der Union im Bereich der Cybersicherheit stellen, bedarf es eines umfassenden Maßnahmenpakets, das auf den bisherigen Maßnahmen der Union aufbaut und sich wechselseitig verstärkende Ziele unterstützt. Dies beinhaltet eine weitere Stärkung der Fähigkeiten und der Abwehrbereitschaft der Mitgliedstaaten und Unternehmen sowie eine bessere Zusammenarbeit und Koordinierung zwischen den Mitgliedstaaten und den Organen, Einrichtungen und Stellen der EU. Da Cyberbedrohungen an keinen Grenzen Halt machen, gilt es zudem, die Fähigkeiten auf Unionsebene zu stärken, die einzelstaatliche Maßnahmen vor allem dann ergänzen könnten, wenn es sich um grenzüberschreitende Cybersicherheitsvorfälle und -krisen von großem Ausmaß handelt. Darüber hinaus sind weitere Anstrengungen notwendig, um die Bürgerinnen und Bürger sowie die Unternehmen für Fragen der Cybersicherheit zu sensibilisieren. Ferner ließe sich das Vertrauen ***in Anbieter digitaler Dienste und*** in den digitalen Binnenmarkt ***als solchen, das durch Cybersicherheitsvorfälle insbesondere unter den Verbrauchern untergraben***

Erleichtert werden kann dies durch eine Zertifizierung, für die über nationale Märkte und Sektoren hinaus unionsweit einheitliche Anforderungen und Bewertungskriterien für die Cybersicherheit festgelegt werden.

wird, weiter erhöhen, wenn transparente Informationen über das Niveau der Sicherheit von IKT-Produkten und -Diensten zur Verfügung stünden. Erleichtert werden kann dies durch eine Zertifizierung, für die über nationale Märkte und Sektoren hinaus unionsweit einheitliche Anforderungen und Bewertungskriterien für die Cybersicherheit festgelegt werden. ***Neben der unionsweiten Zertifizierung stehen verschiedene freiwillige Maßnahmen zur Verfügung, die der Privatsektor ergreifen sollte, um das Vertrauen in die Sicherheit von IKT-Produkten und -Diensten zu stärken, insbesondere im Hinblick auf die zunehmende Verfügbarkeit von IoT-Geräten. So sollten beispielsweise Verschlüsselungs- und andere Technologien sowie Technologien zur erfolgreichen Verhinderung von Cyberangriffen effektiver genutzt werden, um die Sicherheit der Daten und Mitteilungen von Endkunden sowie die gesamte Sicherheit von Netzwerken und Informationssystemen in der Union zu verbessern.***

Or. en

Änderungsantrag 60 **Jiří Maštálka**

Vorschlag für eine Verordnung **Erwägung 5**

Vorschlag der Kommission

(5) Angesichts immer größerer Herausforderungen, die sich der Union im Bereich der Cybersicherheit stellen, bedarf es eines umfassenden Maßnahmenpakets, das auf den bisherigen Maßnahmen der Union aufbaut und sich wechselseitig verstärkende Ziele unterstützt. Dies beinhaltet eine weitere Stärkung der Fähigkeiten und der Abwehrbereitschaft

Geänderter Text

(5) Angesichts immer größerer Herausforderungen, die sich der Union im Bereich der Cybersicherheit stellen, bedarf es eines umfassenden Maßnahmenpakets, das auf den bisherigen Maßnahmen der Union aufbaut und sich wechselseitig verstärkende Ziele unterstützt. Dies beinhaltet eine weitere Stärkung der Fähigkeiten und der Abwehrbereitschaft

der Mitgliedstaaten und Unternehmen sowie eine bessere Zusammenarbeit und Koordinierung zwischen den Mitgliedstaaten und den Organen, Einrichtungen und Stellen der EU. Da Cyberbedrohungen an keinen Grenzen Halt machen, gilt es zudem, die Fähigkeiten auf Unionsebene zu stärken, die einzelstaatliche Maßnahmen vor allem dann ergänzen könnten, wenn es sich um grenzüberschreitende Cybersicherheitsvorfälle und -krisen von großem Ausmaß handelt. Darüber hinaus sind weitere Anstrengungen notwendig, um die Bürgerinnen und Bürger sowie die Unternehmen für Fragen der Cybersicherheit zu sensibilisieren. Ferner ließe sich das Vertrauen in den digitalen Binnenmarkt weiter erhöhen, wenn transparente Informationen über das Niveau der Sicherheit von IKT-Produkten und -Diensten zur Verfügung stünden. Erleichtert werden kann dies durch eine Zertifizierung, für die über nationale Märkte und Sektoren hinaus unionsweit einheitliche Anforderungen und Bewertungskriterien für die Cybersicherheit festgelegt werden.

der Mitgliedstaaten und Unternehmen sowie eine bessere Zusammenarbeit und Koordinierung zwischen den Mitgliedstaaten und den Organen, Einrichtungen und Stellen der EU. Da Cyberbedrohungen an keinen Grenzen Halt machen, gilt es zudem, die Fähigkeiten auf Unionsebene zu stärken, die einzelstaatliche Maßnahmen vor allem dann ergänzen könnten, wenn es sich um grenzüberschreitende Cybersicherheitsvorfälle und -krisen von großem Ausmaß handelt. Darüber hinaus sind weitere Anstrengungen notwendig, um die Bürgerinnen und Bürger sowie die Unternehmen für Fragen der Cybersicherheit zu sensibilisieren. Ferner ließe sich das Vertrauen in den digitalen Binnenmarkt weiter erhöhen, wenn transparente Informationen über das Niveau der Sicherheit von IKT-Produkten und -Diensten zur Verfügung stünden. Erleichtert werden kann dies durch eine ***auf europäischen und internationalen Standards beruhende*** Zertifizierung, für die über nationale Märkte und Sektoren hinaus unionsweit einheitliche Anforderungen und Bewertungskriterien für die Cybersicherheit festgelegt werden.

Or. en

Änderungsantrag 61 **Philippe Juvin**

Vorschlag für eine Verordnung **Erwägung 5**

Vorschlag der Kommission

(5) Angesichts immer größerer Herausforderungen, die sich der Union im Bereich der Cybersicherheit stellen, bedarf es eines umfassenden Maßnahmenpakets, das auf den bisherigen Maßnahmen der Union aufbaut und sich wechselseitig verstärkende Ziele unterstützt. Dies

Geänderter Text

(5) Angesichts immer größerer Herausforderungen, die sich der Union im Bereich der Cybersicherheit stellen, bedarf es eines umfassenden Maßnahmenpakets, das auf den bisherigen Maßnahmen der Union aufbaut und sich wechselseitig verstärkende Ziele unterstützt. Dies

beinhaltet eine weitere Stärkung der Fähigkeiten und der Abwehrbereitschaft der Mitgliedstaaten und Unternehmen sowie eine bessere Zusammenarbeit und Koordinierung zwischen den Mitgliedstaaten und den Organen, Einrichtungen und Stellen der EU. Da Cyberbedrohungen an keinen Grenzen Halt machen, gilt es zudem, die Fähigkeiten auf Unionsebene zu stärken, die einzelstaatliche Maßnahmen vor allem dann ergänzen könnten, wenn es sich um grenzüberschreitende Cybersicherheitsvorfälle und -krisen von großem Ausmaß handelt. Darüber hinaus sind weitere Anstrengungen notwendig, um die Bürgerinnen und Bürger sowie die Unternehmen für Fragen der Cybersicherheit zu sensibilisieren. Ferner ließe sich das Vertrauen in den digitalen Binnenmarkt weiter erhöhen, wenn transparente Informationen über das Niveau der Sicherheit von IKT-Produkten und -Diensten zur Verfügung stünden. Erleichtert werden kann dies durch eine Zertifizierung, für die über nationale Märkte und Sektoren hinaus unionsweit einheitliche Anforderungen und Bewertungskriterien für die Cybersicherheit festgelegt werden.

beinhaltet eine weitere Stärkung der Fähigkeiten und der Abwehrbereitschaft der Mitgliedstaaten und Unternehmen sowie eine bessere Zusammenarbeit und Koordinierung zwischen den Mitgliedstaaten und den Organen, Einrichtungen und Stellen der EU. Da Cyberbedrohungen an keinen Grenzen Halt machen, gilt es zudem, die Fähigkeiten auf Unionsebene zu stärken, die einzelstaatliche Maßnahmen vor allem dann ergänzen könnten, wenn es sich um grenzüberschreitende Cybersicherheitsvorfälle und -krisen von großem Ausmaß handelt. Darüber hinaus sind weitere Anstrengungen notwendig, um die Bürgerinnen und Bürger sowie die Unternehmen für Fragen der Cybersicherheit zu sensibilisieren. Ferner ließe sich das Vertrauen in den digitalen Binnenmarkt weiter erhöhen, wenn transparente Informationen über das Niveau der Sicherheit von IKT-Produkten und -Diensten zur Verfügung stünden. Erleichtert werden kann dies durch eine Zertifizierung, für die *in homogener Weise* über nationale Märkte und Sektoren hinaus unionsweit einheitliche Anforderungen und Bewertungskriterien für die Cybersicherheit festgelegt werden.

Or. fr

Änderungsantrag 62
Maria Grapini

Vorschlag für eine Verordnung
Erwägung 5 a (neu)

Vorschlag der Kommission

Geänderter Text

(5a) Cybersicherheit gegen Cyberangriffe ist eine Dimension der allgemeinen Sicherheit und Kompetenz und Erfahrung hinsichtlich der Risikobewertung sind Sache der Mitgliedstaaten. Die Union teilt sich zwar

die Zuständigkeit im Bereich Freiheit, Sicherheit und Recht mit den Mitgliedstaaten (Artikel 4 AEUV), aber in Anbetracht der Bedeutung von Cybersicherheit für die nationale Sicherheit ist das in vielerlei Hinsicht eine Frage der nationalen Souveränität. Aus diesem Grund, was den einheitlichen europäischen Zertifizierungsrahmen betrifft, sollte die Rolle der Mitgliedstaaten und gleichzeitig die der nationalen Zertifizierungsbehörden nicht nur auf eine beratende Funktion reduziert werden, die Mitgliedstaaten sollten vielmehr auch aufgrund ihrer Erfahrung eine wesentliche Rolle in der neuen Architektur der Zertifizierung der Cybersicherheit spielen.

Or. ro

Änderungsantrag 63
Antanas Guoga

Vorschlag für eine Verordnung
Erwägung 5 a (neu)

Vorschlag der Kommission

Geänderter Text

(5a) Zertifizierungen und andere Formen der Konformitätsbewertung für IKT-Produkte, -Dienste und -Prozesse sind zwar wichtig, für eine Verbesserung der Cybersicherheit ist jedoch ein vielschichtiger Ansatz erforderlich, der Menschen, Prozesse und Technologien umfasst. Ebenso muss die EU weiterhin andere Anstrengungen in den Mittelpunkt stellen und fördern wie die Aufklärung über Cybersicherheit, Schulungen und die Entwicklung von Fertigkeiten in diesem Bereich, Sensibilisierung der Geschäftsführungs- und Vorstandsebene von Unternehmen, Förderung des freiwilligen Informationsaustauschs über Cyber-Bedrohungen und Übergang von

*einem reaktiven zu einem proaktiven
Ansatz bei der Antwort auf Bedrohungen
mit Betonung auf der Prävention
erfolgreicher Cyberangriffe.*

Or. en

Änderungsantrag 64
Philippe Juvin

Vorschlag für eine Verordnung
Erwägung 11

Vorschlag der Kommission

(11) Angesichts der zunehmenden Herausforderungen, mit denen die Union im Bereich der Cybersicherheit konfrontiert ist, sollten die Mittelzuweisungen für die Agentur erhöht werden, damit ihre finanzielle und personelle Ausstattung ihrer größeren Rolle und ihren umfangreicheren Aufgaben sowie ihrer wichtigen Stellung im Kreise der Organisationen gerecht werden kann, die das digitale Ökosystem der EU verteidigen.

Geänderter Text

(11) Angesichts der zunehmenden **Gefahren und** Herausforderungen, mit denen die Union im Bereich der Cybersicherheit konfrontiert ist, sollten die Mittelzuweisungen für die Agentur erhöht werden, damit ihre finanzielle und personelle Ausstattung ihrer größeren Rolle und ihren umfangreicheren Aufgaben sowie ihrer wichtigen Stellung im Kreise der Organisationen gerecht werden kann, die das digitale Ökosystem der EU verteidigen.

Or. fr

Änderungsantrag 65
Maria Grapini

Vorschlag für eine Verordnung
Erwägung 21 a (neu)

Vorschlag der Kommission

(21a) Ersucht die Kommission, Bestimmungen verpflichtender Kooperation zwischen den Mitgliedstaaten zum Schutz kritischer Infrastrukturen zu schaffen.

Or. ro

Änderungsantrag 66
Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Erwägung 28

Vorschlag der Kommission

(28) Die Agentur sollte dabei mitwirken, die Öffentlichkeit für Cybersicherheitsrisiken zu sensibilisieren, und Leitlinien für bewährte Verfahren zur Verfügung stellen, die sich an Bürger sowie an Organisationen wenden. Darüber hinaus sollte die Agentur einen Beitrag dazu leisten, bewährte Verfahren und Lösungen auf der Ebene von Einzelpersonen und Organisationen zu fördern, indem sie öffentlich verfügbare Informationen über erhebliche Sicherheitsvorfälle sammelt und analysiert und Berichte hierüber erstellt, die Unternehmen und Bürgern als Leitfaden dienen können und die das Niveau der Abwehrbereitschaft und Abwehrfähigkeit insgesamt erhöhen. Ferner sollte die Agentur in Zusammenarbeit mit den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU regelmäßige öffentliche Aufklärungskampagnen durchführen, die sich an die Endnutzer richten und zum Ziel haben, sicherere Verhaltensweisen der Nutzer im Internet zu fördern, die Nutzer für potenzielle Bedrohungen im Internet – auch für die Cyberkriminalität wie das Abgreifen von Daten (Phishing), Botnets, Finanz- und Bankenbetrug – stärker zu sensibilisieren und einfache Empfehlungen in Bezug auf **Authentifizierung** und Datenschutz zu geben. Die Agentur sollte eine zentrale Rolle dabei spielen, die Sensibilisierung der Endnutzer für die Sicherheit von Geräten zu forcieren.

Geänderter Text

(28) Die Agentur sollte dabei mitwirken, die Öffentlichkeit für Cybersicherheitsrisiken zu sensibilisieren, und Leitlinien für bewährte Verfahren zur Verfügung stellen, die sich an Bürger sowie an Organisationen wenden. Darüber hinaus sollte die Agentur einen Beitrag dazu leisten, bewährte Verfahren und Lösungen **im Bereich der Cyberhygiene** auf der Ebene von Einzelpersonen und Organisationen zu fördern, indem sie öffentlich verfügbare Informationen über erhebliche Sicherheitsvorfälle sammelt und analysiert und Berichte hierüber erstellt, die Unternehmen und Bürgern als Leitfaden dienen können und die das Niveau der Abwehrbereitschaft und Abwehrfähigkeit insgesamt erhöhen. Ferner sollte die Agentur in Zusammenarbeit mit den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU regelmäßige öffentliche Aufklärungskampagnen durchführen, die sich an die Endnutzer richten und zum Ziel haben, sicherere Verhaltensweisen der Nutzer im Internet zu fördern, die Nutzer für potenzielle Bedrohungen im Internet – auch für die Cyberkriminalität wie das Abgreifen von Daten (Phishing), Botnets, Finanz- und Bankenbetrug – stärker zu sensibilisieren und einfache Empfehlungen in Bezug auf **Multi-Faktor-Authentifizierung, Fehlerkorrektur, Verschlüsselung, Grundsätze des Zugriffsmanagements** und Datenschutz zu geben. Die Agentur sollte eine zentrale Rolle dabei spielen, die Sensibilisierung der Endnutzer für die Sicherheit von Geräten zu forcieren. **Die**

Agentur sollte alle Endnutzer dazu ermutigen, angemessene Maßnahmen zur Verhinderung und Minimierung der Auswirkungen von Vorfällen, die die Sicherheit ihrer Netze und Informationssysteme betreffen, zu ergreifen.

Or. en

Änderungsantrag 67
Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung
Erwägung 28

Vorschlag der Kommission

(28) Die Agentur sollte dabei mitwirken, die Öffentlichkeit für **Cybersicherheitsrisiken** zu sensibilisieren, und Leitlinien für bewährte Verfahren zur Verfügung stellen, die sich an Bürger sowie an Organisationen wenden. Darüber hinaus sollte die Agentur einen Beitrag dazu leisten, bewährte Verfahren und Lösungen auf der Ebene von Einzelpersonen und Organisationen zu fördern, indem sie öffentlich verfügbare Informationen über erhebliche Sicherheitsvorfälle sammelt und analysiert und Berichte hierüber erstellt, die Unternehmen und Bürgern als Leitfaden dienen können und die das Niveau der Abwehrbereitschaft und Abwehrfähigkeit insgesamt erhöhen. Ferner sollte die Agentur in Zusammenarbeit mit den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU regelmäßige öffentliche Aufklärungskampagnen durchführen, die sich an die Endnutzer richten und zum Ziel haben, sicherere Verhaltensweisen der Nutzer im Internet zu fördern, die Nutzer für potenzielle Bedrohungen im Internet – auch für die Cyberkriminalität wie das

Geänderter Text

(28) Die Agentur sollte dabei mitwirken, die Öffentlichkeit für **IT-Sicherheitsrisiken** zu sensibilisieren, und Leitlinien für bewährte Verfahren zur Verfügung stellen, die sich an Bürger sowie an Organisationen wenden. Darüber hinaus sollte die Agentur einen Beitrag dazu leisten, bewährte Verfahren und Lösungen auf der Ebene von Einzelpersonen und Organisationen zu fördern, indem sie öffentlich verfügbare Informationen über erhebliche Sicherheitsvorfälle sammelt und analysiert und Berichte **und Ratgeber** hierüber erstellt **und veröffentlicht**, die Unternehmen und Bürgern als Leitfaden dienen können und die das Niveau der Abwehrbereitschaft und Abwehrfähigkeit insgesamt erhöhen. Ferner sollte die Agentur in Zusammenarbeit mit den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU regelmäßige öffentliche Aufklärungskampagnen durchführen, die sich an die Endnutzer richten und zum Ziel haben, sicherere Verhaltensweisen der Nutzer im Internet zu fördern, die Nutzer für potenzielle Bedrohungen im Internet –

Abgreifen von Daten (Phishing), Botnets, Finanz- und Bankenbetrug – stärker zu sensibilisieren und einfache Empfehlungen in Bezug auf Authentifizierung und Datenschutz zu geben. Die Agentur sollte eine zentrale Rolle dabei spielen, die Sensibilisierung der Endnutzer für die Sicherheit von Geräten zu forcieren.

auch für die Cyberkriminalität wie das Abgreifen von Daten (Phishing), Botnets, Finanz- und Bankenbetrug – stärker zu sensibilisieren und einfache Empfehlungen in Bezug auf Authentifizierung, ***Verschlüsselung, Anonymisierung*** und Datenschutz zu geben. Die Agentur sollte eine zentrale Rolle dabei spielen, die Sensibilisierung der Endnutzer für die Sicherheit von Geräten zu forcieren ***und eingebaute Sicherheit und Privatsphäre sowie die Vorfälle und deren Lösungen auf EU-Ebene bekannt zu machen.***

Or. en

Begründung

Die Ziele werden im Einklang mit dem Inhalt der Artikel aufgeführt.

Änderungsantrag 68 **Anneleen Van Bossuyt, Daniel Dalton**

Vorschlag für eine Verordnung **Erwägung 28**

Vorschlag der Kommission

(28) Die Agentur sollte dabei mitwirken, die Öffentlichkeit für Cybersicherheitsrisiken zu sensibilisieren, und Leitlinien für bewährte Verfahren zur Verfügung stellen, die sich an Bürger sowie an Organisationen wenden. Darüber hinaus sollte die Agentur einen Beitrag dazu leisten, bewährte Verfahren und Lösungen auf der Ebene von Einzelpersonen und Organisationen zu fördern, indem sie öffentlich verfügbare Informationen über erhebliche Sicherheitsvorfälle sammelt und analysiert und Berichte hierüber erstellt, die Unternehmen und Bürgern als Leitfaden dienen können und die das Niveau der Abwehrbereitschaft und Abwehrfähigkeit insgesamt erhöhen. Ferner sollte die Agentur in Zusammenarbeit mit den

Geänderter Text

(28) Die Agentur sollte dabei mitwirken, die Öffentlichkeit für Cybersicherheitsrisiken zu sensibilisieren, und Leitlinien für bewährte Verfahren zur Verfügung stellen, die sich an Bürger sowie an Organisationen wenden. Darüber hinaus sollte die Agentur einen Beitrag dazu leisten, bewährte Verfahren und Lösungen auf der Ebene von Einzelpersonen und Organisationen zu fördern, indem sie öffentlich verfügbare Informationen über erhebliche Sicherheitsvorfälle sammelt und analysiert und Berichte hierüber erstellt, die Unternehmen und Bürgern als Leitfaden dienen können und die das Niveau der Abwehrbereitschaft und Abwehrfähigkeit insgesamt erhöhen. Ferner sollte die Agentur in Zusammenarbeit mit den

Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU regelmäßige öffentliche Aufklärungskampagnen durchführen, die sich an die Endnutzer richten und zum Ziel haben, sicherere Verhaltensweisen der Nutzer im Internet zu fördern, die Nutzer für *potenzielle* Bedrohungen im Internet – auch für die Cyberkriminalität wie das Abgreifen von Daten (Phishing), Botnets, Finanz- und Bankenbetrug – stärker zu sensibilisieren und einfache Empfehlungen in Bezug auf Authentifizierung und Datenschutz zu geben. Die Agentur sollte eine zentrale Rolle dabei spielen, die Sensibilisierung der Endnutzer für die Sicherheit von Geräten zu forcieren.

Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU regelmäßige öffentliche Aufklärungskampagnen durchführen, die sich an die Endnutzer richten und zum Ziel haben, sicherere Verhaltensweisen der Nutzer im Internet zu fördern, die Nutzer für *mögliche Maßnahmen zum Schutz vor potenziellen* Bedrohungen im Internet – auch für die Cyberkriminalität wie das Abgreifen von Daten (Phishing), Botnets, Finanz- und Bankenbetrug – stärker zu sensibilisieren und einfache Empfehlungen in Bezug auf Authentifizierung und Datenschutz zu geben. Die Agentur sollte eine zentrale Rolle dabei spielen, die Sensibilisierung der Endnutzer für die Sicherheit von Geräten *und die sichere Nutzung von Diensten* zu forcieren.

Or. en

Änderungsantrag 69

Liisa Jaakonsaari, Christel Schaldemose, Lucy Anderson, Arndt Kohn

Vorschlag für eine Verordnung

Erwägung 28

Vorschlag der Kommission

(28) Die Agentur sollte dabei mitwirken, die Öffentlichkeit für Cybersicherheitsrisiken zu sensibilisieren, und Leitlinien für bewährte Verfahren zur Verfügung stellen, die sich an Bürger sowie an Organisationen wenden. Darüber hinaus sollte die Agentur einen Beitrag dazu leisten, bewährte Verfahren und Lösungen auf der Ebene von Einzelpersonen und Organisationen zu fördern, indem sie öffentlich verfügbare Informationen über erhebliche Sicherheitsvorfälle sammelt und analysiert und Berichte hierüber erstellt, die Unternehmen und Bürgern als Leitfaden dienen können und die das Niveau der Abwehrbereitschaft und Abwehrfähigkeit

Geänderter Text

(28) Die Agentur sollte dabei mitwirken, die Öffentlichkeit für Cybersicherheitsrisiken zu sensibilisieren, und Leitlinien für bewährte Verfahren zur Verfügung stellen, die sich an Bürger sowie an Organisationen wenden. Darüber hinaus sollte die Agentur einen Beitrag dazu leisten, bewährte Verfahren und Lösungen auf der Ebene von Einzelpersonen und Organisationen zu fördern, indem sie öffentlich verfügbare Informationen über erhebliche Sicherheitsvorfälle sammelt und analysiert und Berichte hierüber erstellt, die Unternehmen und Bürgern als Leitfaden dienen können und die das Niveau der Abwehrbereitschaft und Abwehrfähigkeit

insgesamt erhöhen. Ferner sollte die Agentur in Zusammenarbeit mit den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU regelmäßige öffentliche Aufklärungskampagnen durchführen, die sich an die Endnutzer richten und zum Ziel haben, sicherere Verhaltensweisen der Nutzer im Internet zu fördern, die Nutzer für potenzielle Bedrohungen im Internet – auch für die Cyberkriminalität wie das Abgreifen von Daten (Phishing), Botnets, Finanz- und Bankenbetrug – stärker zu sensibilisieren und einfache Empfehlungen in Bezug auf Authentifizierung und Datenschutz zu geben. Die Agentur sollte eine zentrale Rolle dabei spielen, die Sensibilisierung der Endnutzer für die Sicherheit von Geräten zu forcieren.

insgesamt erhöhen. Ferner sollte die Agentur in Zusammenarbeit mit den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der EU regelmäßige öffentliche Aufklärungskampagnen durchführen, die sich an die Endnutzer richten und zum Ziel haben, sicherere Verhaltensweisen der Nutzer im Internet zu fördern, die Nutzer für potenzielle Bedrohungen im Internet – auch für die Cyberkriminalität wie das Abgreifen von Daten (Phishing), **Ransomware-Angriffe, das Kapern von Geräten**, Botnets, Finanz- und Bankenbetrug – stärker zu sensibilisieren und einfache Empfehlungen in Bezug auf Authentifizierung und Datenschutz zu geben. Die Agentur sollte eine zentrale Rolle dabei spielen, die Sensibilisierung der Endnutzer für die Sicherheit von Geräten zu forcieren.

Or. en

Änderungsantrag 70

Liisa Jaakonsaari, Christel Schaldemose, Lucy Anderson, Arndt Kohn

Vorschlag für eine Verordnung Erwägung 28 a (neu)

Vorschlag der Kommission

Geänderter Text

(28a) Die Agentur sollte die generelle Berücksichtigung des Grundsatzes der eingebauten Sicherheit fördern, der für die Verbesserung der Sicherheit vernetzter Geräte von entscheidender Bedeutung ist. Das Prinzip der eingebauten Sicherheit ist besonders für Geräte wichtig, die für schutzbedürftige Endnutzer wie Kinder bestimmt sind.

Or. en

Änderungsantrag 71

Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung
Erwägung 30

Vorschlag der Kommission

(30) Damit die Agentur ihre Ziele in vollem Umfang verwirklichen kann, sollte sie zu den einschlägigen Organen, Einrichtungen und sonstigen Stellen der EU Kontakt halten – etwa zum CERT-EU, zum Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) bei Europol, zur Europäischen Verteidigungsagentur (EDA), zur Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen (eu-LISA), zur Europäischen Agentur für Flugsicherheit (EASA) und zu sonstigen EU-Agenturen, die sich mit Fragen der **Cybersicherheit** beschäftigen. Für den Austausch von Know-how und bewährten Verfahren und für die Beratung zu Aspekten der **Cybersicherheit**, die sich auf die Arbeit von Datenschutzbehörden auswirken können, sollte die Agentur auch mit diesen in Verbindung stehen. Vertreter der Strafverfolgungs- und der Datenschutzbehörden auf nationaler Ebene und auf Unionsebene sollten als Vertreter für eine Mitwirkung in der Ständigen Gruppe der Interessenträger der Agentur in Frage kommen. Bei ihren Kontakten mit Strafverfolgungsbehörden in Bezug auf Netz- und Informationssicherheitsaspekte, die sich möglicherweise auf deren Arbeit auswirken, sollte die Agentur vorhandene Informationskanäle und bestehende Netze beachten.

Geänderter Text

(30) Damit die Agentur ihre Ziele in vollem Umfang verwirklichen kann, sollte sie zu den einschlägigen Organen, Einrichtungen und sonstigen Stellen der EU Kontakt halten – etwa zum CERT-EU, zum Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) bei Europol, zur Europäischen Verteidigungsagentur (EDA), zur Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen (eu-LISA), zur Europäischen Agentur für Flugsicherheit (EASA) und zu sonstigen EU-Agenturen, die sich mit Fragen der **IT-Sicherheit** beschäftigen. Für den Austausch von Know-how und bewährten Verfahren und für die Beratung zu Aspekten der **IT-Sicherheit**, die sich auf die Arbeit von Datenschutzbehörden auswirken können, sollte die Agentur auch mit diesen in Verbindung stehen. Vertreter der Strafverfolgungs- und der Datenschutzbehörden auf nationaler Ebene und auf Unionsebene sollten als Vertreter für eine Mitwirkung in der Ständigen Gruppe der Interessenträger der Agentur in Frage kommen. Bei ihren Kontakten mit Strafverfolgungsbehörden in Bezug auf Netz- und Informationssicherheitsaspekte, die sich möglicherweise auf deren Arbeit auswirken, sollte die Agentur vorhandene Informationskanäle und bestehende Netze beachten. ***Es sollten Partnerschaften mit Hochschulen gegründet werden, die in den betreffenden Bereichen Forschungsinitiativen haben. Für Beiträge von Verbraucherschutzverbänden und anderen Organisationen, die stets analysiert werden sollten, sollten***

wiederum geeignete Kanäle zur Verfügung stehen.

Or. en

Begründung

Einführung der Auffassung, dass die ENISA vom Pool des vorhandenen Wissens profitieren sollte.

Änderungsantrag 72
Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Erwägung 33

Vorschlag der Kommission

(33) *Die Agentur sollte ihre Sachkenntnis im Bereich der Cybersicherheitszertifizierung weiter ausbauen und pflegen, damit sie die Unionspolitik auf diesem Gebiet unterstützen kann.* Die Agentur sollte die Nutzung der *Cybersicherheitszertifizierung in der Union* fördern, *auch indem sie* zum Aufbau und zur Pflege eines Cybersicherheitszertifizierungsrahmens auf Unionsebene *beiträgt*, um so die auf mehr Transparenz gestützte Vertrauenswürdigkeit der Cybersicherheit von IKT-Produkten und -Diensten zu erhöhen und damit das Vertrauen in den digitalen Binnenmarkt zu stärken.

Geänderter Text

(33) Die Agentur sollte die Nutzung der *Zertifizierung fördern und die Fragmentierung, die durch einen Mangel an Koordinierung zwischen vorhandenen Zertifizierungssystemen in der Union entsteht, vermeiden.* *Die Agentur sollte* zum Aufbau und zur Pflege eines Cybersicherheitszertifizierungsrahmens auf Unionsebene *im Sinne der Artikel 43 bis 54 [Titel III] beitragen*, um so die auf mehr Transparenz gestützte Vertrauenswürdigkeit der Cybersicherheit von IKT-Produkten und -Diensten zu erhöhen und damit das Vertrauen in den digitalen Binnenmarkt zu stärken.

Or. en

Änderungsantrag 73
Liisa Jaakonsaari, Lucy Anderson

Vorschlag für eine Verordnung
Erwägung 35

Vorschlag der Kommission

(35) Die Agentur sollte die Mitgliedstaaten und die Diensteanbieter dazu anspornen, ihre allgemeinen Sicherheitsstandards zu heben, damit alle Internetnutzer die erforderlichen Vorkehrungen für ihre persönliche Cybersicherheit treffen können. So sollten Diensteanbieter und Produkthersteller diese Dienste und Produkte vom Markt nehmen oder umrüsten, wenn sie den Cybersicherheitsstandards nicht genügen. In Zusammenarbeit mit den zuständigen Behörden kann die ENISA Informationen über das Niveau der Cybersicherheit von Produkten und Diensten verbreiten, die auf dem Binnenmarkt angeboten werden, Anbieter und Hersteller verwarnen und sie auffordern, die Sicherheit, auch die Cybersicherheit, ihrer Produkte und Dienste zu verbessern.

Geänderter Text

(35) Die Agentur sollte die Mitgliedstaaten und die Diensteanbieter dazu anspornen, ihre allgemeinen Sicherheitsstandards zu heben, damit alle Internetnutzer die erforderlichen Vorkehrungen für ihre persönliche Cybersicherheit treffen können. So sollten Diensteanbieter und Produkthersteller diese Dienste und Produkte vom Markt nehmen oder umrüsten, wenn sie den Cybersicherheitsstandards nicht genügen. In Zusammenarbeit mit den zuständigen Behörden kann die ENISA Informationen über das Niveau der Cybersicherheit von Produkten und Diensten verbreiten, die auf dem Binnenmarkt angeboten werden, Anbieter und Hersteller verwarnen und sie auffordern, die Sicherheit, auch die Cybersicherheit, ihrer Produkte und Dienste zu verbessern. ***Alle Anbieter oder Hersteller, die eine Verwarnung bezüglich des Niveaus der Cybersicherheit ihrer Produkte erhalten, sollten in einem speziellen Portal öffentlich gemacht werden.***

Or. en

Änderungsantrag 74

Jan Philipp Albrecht

im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung

Erwägung 35

Vorschlag der Kommission

(35) Die Agentur sollte die Mitgliedstaaten und die Diensteanbieter dazu anspornen, ihre allgemeinen Sicherheitsstandards zu heben, damit alle Internetnutzer die erforderlichen Vorkehrungen für ihre persönliche ***Cybersicherheit*** treffen können. So sollten Diensteanbieter und Produkthersteller diese

Geänderter Text

(35) Die Agentur sollte die Mitgliedstaaten und die Diensteanbieter dazu anspornen, ihre allgemeinen Sicherheitsstandards zu heben, damit alle Internetnutzer die erforderlichen Vorkehrungen für ihre persönliche ***IT-Sicherheit*** treffen können, ***und den Verkauf oder die Nutzung von Geräten***

Dienste und Produkte vom Markt nehmen oder umrüsten, wenn sie den **Cybersicherheitsstandards** nicht genügen. In Zusammenarbeit mit den zuständigen Behörden kann die ENISA Informationen über das Niveau der **Cybersicherheit** von Produkten und Diensten verbreiten, die auf dem Binnenmarkt angeboten werden, Anbieter und Hersteller verwarnen und sie auffordern, die Sicherheit, auch die **Cybersicherheit**, ihrer Produkte und Dienste zu verbessern.

nicht zu erlauben, die die Mindestsicherheitsbedingungen nicht erfüllen. So sollten Diensteanbieter und Produkthersteller diese Dienste und Produkte vom Markt nehmen oder umrüsten, wenn sie den **IT-Sicherheitsstandards** nicht genügen. In Zusammenarbeit mit den zuständigen Behörden kann die ENISA Informationen über das Niveau der **IT-Sicherheit** von Produkten und Diensten verbreiten, die auf dem Binnenmarkt angeboten werden, Anbieter und Hersteller verwarnen und sie auffordern, die Sicherheit, auch die **IT-Sicherheit**, ihrer Produkte und Dienste zu verbessern.

Or. en

Begründung

Gemäß der Einführung einer Grundanforderung im Bereich der IT-Sicherheit

Änderungsantrag 75

Jan Philipp Albrecht

im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung

Erwägung 41

Vorschlag der Kommission

(41) Damit die Agentur ihre Aufgaben ordnungsgemäß und effizient wahrnehmen kann, sollten die Kommission und die Mitgliedstaaten sicherstellen, dass die Personen, die als Mitglieder des Verwaltungsrats ernannt werden, über angemessenes Fachwissen und Erfahrung in Funktionsbereichen verfügen. Die Kommission und die Mitgliedstaaten sollten sich auch darum bemühen, die Fluktuation bei ihren jeweiligen Vertretern im Verwaltungsrat zu verringern, um die Kontinuität seiner Arbeit sicherzustellen.

Geänderter Text

(41) Damit die Agentur ihre Aufgaben ordnungsgemäß und effizient wahrnehmen kann, sollten die Kommission und die Mitgliedstaaten sicherstellen, dass die Personen, die als Mitglieder des Verwaltungsrats ernannt werden, über angemessenes Fachwissen und Erfahrung in Funktionsbereichen verfügen. Die Kommission und die Mitgliedstaaten sollten sich auch darum bemühen, die Fluktuation bei ihren jeweiligen Vertretern im Verwaltungsrat zu verringern, um die Kontinuität seiner Arbeit sicherzustellen. ***Aufgrund des hohen Marktwerts der für die Arbeit der Agentur erforderlichen***

Fertigkeiten muss dafür gesorgt werden, dass die Gehälter und die sozialen Bedingungen für alle Mitarbeiter der Agentur wettbewerbsfähig sind, damit sichergestellt ist, dass die besten Experten sich für eine Arbeit in der Agentur entscheiden können.

Or. en

Begründung

Um ein angemessenes Niveau an Sachkenntnis zu erhalten, muss die ENISA auf einem hart umkämpften Markt eine wettbewerbsfähige Arbeitgeberin sein.

Änderungsantrag 76
Mylène Troszczyński

Vorschlag für eine Verordnung
Erwägung 41

Vorschlag der Kommission

(41) Damit die Agentur ihre Aufgaben ordnungsgemäß und effizient wahrnehmen kann, sollten **die Kommission und** die Mitgliedstaaten sicherstellen, dass die Personen, die als Mitglieder des Verwaltungsrats ernannt werden, über angemessenes Fachwissen und Erfahrung in Funktionsbereichen verfügen. **Die Kommission und die Mitgliedstaaten sollten sich auch darum bemühen, die Fluktuation bei ihren jeweiligen Vertretern im Verwaltungsrat zu verringern, um die Kontinuität seiner Arbeit sicherzustellen.**

Geänderter Text

(41) Damit die Agentur ihre Aufgaben ordnungsgemäß und effizient wahrnehmen kann, sollten die Mitgliedstaaten sicherstellen, dass die Personen, die als Mitglieder des Verwaltungsrats ernannt werden, über angemessenes Fachwissen und Erfahrung in Funktionsbereichen verfügen.

Or. fr

Änderungsantrag 77
Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung

Erwägung 42

Vorschlag der Kommission

(42) Damit die Agentur reibungslos funktioniert, ist es erforderlich, dass ihr Exekutivdirektor aufgrund seiner Verdienste und nachgewiesenen Verwaltungs- und Managementfähigkeiten ernannt wird, über einschlägige Sachkenntnis und Erfahrungen auf dem Gebiet der **Cybersicherheit** verfügt und seine Aufgaben völlig unabhängig wahrnimmt. Der Exekutivdirektor sollte nach Anhörung der Kommission einen Vorschlag für das Arbeitsprogramm der Agentur ausarbeiten und alle erforderlichen Maßnahmen zu dessen ordnungsgemäßer Durchführung ergreifen. Der Exekutivdirektor sollte einen Jahresbericht ausarbeiten, der dem Verwaltungsrat vorgelegt wird, den Entwurf eines Voranschlags für die Einnahmen und Ausgaben der Agentur erstellen und den Haushaltsplan ausführen. Der Exekutivdirektor sollte zudem die Möglichkeit haben, Ad-hoc-Arbeitsgruppen einzusetzen, die sich mit wissenschaftlichen, technischen, rechtlichen oder wirtschaftlichen Einzelfragen befassen. Der Exekutivdirektor sollte dafür sorgen, dass die Mitglieder der Ad-hoc-Arbeitsgruppen höchsten fachlichen Ansprüchen genügen und dass je nach Einzelfrage gegebenenfalls ein repräsentatives Gleichgewicht zwischen öffentlichen Verwaltungen der Mitgliedstaaten, den Organen der Union und dem Privatsektor einschließlich der Wirtschaft, der Nutzer und wissenschaftlicher Sachverständiger für Netz- und Informationssicherheit gewahrt wird.

Geänderter Text

(42) Damit die Agentur reibungslos funktioniert, ist es erforderlich, dass ihr Exekutivdirektor aufgrund seiner Verdienste und nachgewiesenen Verwaltungs- und Managementfähigkeiten ernannt wird, über einschlägige Sachkenntnis und Erfahrungen auf dem Gebiet der **IT-Sicherheit** verfügt und seine Aufgaben völlig unabhängig wahrnimmt. Der Exekutivdirektor sollte nach Anhörung der Kommission einen Vorschlag für das Arbeitsprogramm der Agentur ausarbeiten und alle erforderlichen Maßnahmen zu dessen ordnungsgemäßer Durchführung ergreifen. Der Exekutivdirektor sollte einen Jahresbericht ausarbeiten, der dem Verwaltungsrat vorgelegt wird, den Entwurf eines Voranschlags für die Einnahmen und Ausgaben der Agentur erstellen und den Haushaltsplan ausführen. Der Exekutivdirektor sollte zudem die Möglichkeit haben, Ad-hoc-Arbeitsgruppen einzusetzen, die sich mit wissenschaftlichen, technischen, rechtlichen oder wirtschaftlichen Einzelfragen befassen. Der Exekutivdirektor sollte dafür sorgen, dass die Mitglieder der Ad-hoc-Arbeitsgruppen höchsten fachlichen Ansprüchen genügen und dass je nach Einzelfrage gegebenenfalls ein repräsentatives Gleichgewicht zwischen öffentlichen Verwaltungen der Mitgliedstaaten, den Organen der Union und dem Privatsektor einschließlich der Wirtschaft, der Nutzer und wissenschaftlicher Sachverständiger für Netz- und Informationssicherheit **sowie ein ausgewogenes Verhältnis von Frauen und Männern** gewahrt wird.

Or. en

Begründung

Einführung von Änderungen zur Herstellung des Gleichgewichts zwischen Männern und

Änderungsantrag 78
Mylène Troszczynski

Vorschlag für eine Verordnung
Erwägung 42

Vorschlag der Kommission

(42) Damit die Agentur reibungslos funktioniert, ist es erforderlich, dass ihr Exekutivdirektor aufgrund seiner Verdienste und nachgewiesenen Verwaltungs- und Managementfähigkeiten ernannt wird, über einschlägige Sachkenntnis und Erfahrungen auf dem Gebiet der Cybersicherheit verfügt und seine Aufgaben völlig unabhängig wahrnimmt. Der Exekutivdirektor sollte **nach Anhörung der Kommission** einen Vorschlag für das Arbeitsprogramm der Agentur ausarbeiten und alle erforderlichen Maßnahmen zu dessen ordnungsgemäßer Durchführung ergreifen. Der Exekutivdirektor sollte einen Jahresbericht ausarbeiten, der dem Verwaltungsrat vorgelegt wird, den Entwurf eines Voranschlags für die Einnahmen und Ausgaben der Agentur erstellen und den Haushaltsplan ausführen. Der Exekutivdirektor sollte zudem die Möglichkeit haben, Ad-hoc-Arbeitsgruppen einzusetzen, die sich mit wissenschaftlichen, technischen, rechtlichen oder wirtschaftlichen Einzelfragen befassen. Der Exekutivdirektor sollte dafür sorgen, dass die Mitglieder der Ad-hoc-Arbeitsgruppen höchsten fachlichen Ansprüchen genügen und dass je nach Einzelfrage gegebenenfalls ein repräsentatives Gleichgewicht zwischen öffentlichen Verwaltungen der Mitgliedstaaten, den Organen der Union und dem Privatsektor einschließlich der Wirtschaft, der Nutzer und wissenschaftlicher Sachverständiger

Geänderter Text

(42) Damit die Agentur reibungslos funktioniert, ist es erforderlich, dass ihr Exekutivdirektor aufgrund seiner Verdienste und nachgewiesenen Verwaltungs- und Managementfähigkeiten ernannt wird, über einschlägige Sachkenntnis und Erfahrungen auf dem Gebiet der Cybersicherheit verfügt und seine Aufgaben völlig unabhängig wahrnimmt. Der Exekutivdirektor sollte einen Vorschlag für das Arbeitsprogramm der Agentur ausarbeiten und alle erforderlichen Maßnahmen zu dessen ordnungsgemäßer Durchführung ergreifen. Der Exekutivdirektor sollte einen Jahresbericht ausarbeiten, der dem Verwaltungsrat vorgelegt wird, den Entwurf eines Voranschlags für die Einnahmen und Ausgaben der Agentur erstellen und den Haushaltsplan ausführen. Der Exekutivdirektor sollte zudem die Möglichkeit haben, Ad-hoc-Arbeitsgruppen einzusetzen, die sich mit wissenschaftlichen, technischen, rechtlichen oder wirtschaftlichen Einzelfragen befassen. Der Exekutivdirektor sollte dafür sorgen, dass die Mitglieder der Ad-hoc-Arbeitsgruppen höchsten fachlichen Ansprüchen genügen und dass je nach Einzelfrage gegebenenfalls ein repräsentatives Gleichgewicht zwischen öffentlichen Verwaltungen der Mitgliedstaaten, den Organen der Union und dem Privatsektor einschließlich der Wirtschaft, der Nutzer und wissenschaftlicher Sachverständiger für Netz- und Informationssicherheit

für Netz- und Informationssicherheit
gewahrt wird.

gewahrt wird.

Or. fr

Änderungsantrag 79
Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung
Erwägung 44

Vorschlag der Kommission

(44) Die Agentur sollte über eine Ständige Gruppe der Interessenträger als Beratungsgremium verfügen, um einen regelmäßigen Dialog mit dem Privatsektor, Verbraucherorganisationen und sonstigen Interessenträgern sicherzustellen. Die vom Verwaltungsrat auf Vorschlag des Exekutivdirektors eingesetzte Ständige Gruppe der Interessenträger sollte hauptsächlich Fragen behandeln, die die Beteiligten betreffen, und diese der Agentur zur Kenntnis bringen. Die Zusammensetzung der Ständigen Gruppe der Interessenträger und die dieser Gruppe übertragenen Aufgaben, die vor allem aus dem Entwurf des Arbeitsprogramms hervorgehen, sollten gewährleisten, dass die Interessenträger bei der Tätigkeit der Agentur **ausreichend** vertreten sind.

Geänderter Text

(44) Die Agentur sollte über eine Ständige Gruppe der Interessenträger als Beratungsgremium verfügen, um einen regelmäßigen Dialog mit dem Privatsektor, Verbraucherorganisationen, **Hochschulen** und sonstigen Interessenträgern sicherzustellen. Die vom Verwaltungsrat auf Vorschlag des Exekutivdirektors eingesetzte Ständige Gruppe der Interessenträger sollte hauptsächlich Fragen behandeln, die die Beteiligten betreffen, und diese der Agentur zur Kenntnis bringen **sowie Beiträge dazu leisten, welche IKT-Produkte und -Dienste in zukünftigen europäischen IT-Sicherheitszertifizierungssystemen abgedeckt werden sollten**. Die Zusammensetzung der Ständigen Gruppe der Interessenträger und die dieser Gruppe übertragenen Aufgaben, die vor allem aus dem Entwurf des Arbeitsprogramms hervorgehen, sollten gewährleisten, dass die Interessenträger bei der Tätigkeit der Agentur **wirksam und ausgewogen** vertreten sind.

Or. en

Änderungsantrag 80
Jiří Pospíšil

Vorschlag für eine Verordnung

Erwägung 44

Vorschlag der Kommission

(44) Die Agentur sollte über eine Ständige Gruppe der Interessenträger als Beratungsgremium verfügen, um einen regelmäßigen Dialog mit dem Privatsektor, Verbraucherorganisationen und sonstigen Interessenträgern sicherzustellen. Die vom Verwaltungsrat auf Vorschlag des Exekutivdirektors eingesetzte Ständige Gruppe der Interessenträger sollte hauptsächlich Fragen behandeln, die die Beteiligten **betreffen** und diese der Agentur zur Kenntnis bringen. Die Zusammensetzung der Ständigen Gruppe der Interessenträger und die dieser Gruppe übertragenen Aufgaben, die vor allem aus dem Entwurf des Arbeitsprogramms hervorgehen, sollten gewährleisten, dass die Interessenträger bei der Tätigkeit der Agentur ausreichend vertreten sind.

Geänderter Text

(44) Die Agentur sollte über eine Ständige Gruppe der Interessenträger als Beratungsgremium verfügen, um einen regelmäßigen Dialog mit dem Privatsektor, Verbraucherorganisationen und sonstigen Interessenträgern sicherzustellen. Die vom Verwaltungsrat auf Vorschlag des Exekutivdirektors eingesetzte Ständige Gruppe der Interessenträger sollte hauptsächlich Fragen behandeln, die **für** die Beteiligten **von Bedeutung sind**, und diese der Agentur zur Kenntnis bringen. Die Zusammensetzung der Ständigen Gruppe der Interessenträger und die dieser Gruppe übertragenen Aufgaben, die vor allem aus dem Entwurf des Arbeitsprogramms hervorgehen, sollten gewährleisten, dass die Interessenträger bei der Tätigkeit der Agentur ausreichend vertreten sind.

Or. cs

Änderungsantrag 81

Jiří Pospíšil

Vorschlag für eine Verordnung

Erwägung 46

Vorschlag der Kommission

(46) Damit die volle Autonomie und Unabhängigkeit der Agentur gewährleistet ist und sie zusätzliche und neue Aufgaben – auch nicht vorhergesehene Aufgaben in Notfällen – erfüllen kann, sollte die Agentur über einen ausreichenden und eigenständigen Haushalt verfügen, der hauptsächlich durch einen Beitrag der Union und durch Beiträge von Drittländern, die sich an der Arbeit der Agentur beteiligen, finanziert wird. Die

Geänderter Text

(46) Damit die volle Autonomie und Unabhängigkeit der Agentur gewährleistet ist und sie zusätzliche und neue Aufgaben – auch nicht vorhergesehene Aufgaben in Notfällen – erfüllen kann, sollte die Agentur über einen ausreichenden und eigenständigen Haushalt verfügen, der hauptsächlich durch einen Beitrag der Union und durch Beiträge von Drittländern, die sich an der Arbeit der Agentur beteiligen, finanziert wird. Die

Mehrheit der Agenturbediensteten sollte unmittelbar mit der operativen Umsetzung des Mandats der Agentur befasst sein. Dem Sitzmitgliedstaat und anderen Mitgliedstaaten sollte es erlaubt sein, freiwillige Beiträge zu den Einnahmen der Agentur zu leisten. Sämtliche Zuschüsse aus dem Gesamthaushaltsplan der Europäischen Union sollten dem Haushaltsverfahren der Union unterliegen. Ferner sollte die Rechnungsführung der Agentur durch den Rechnungshof geprüft werden, um **Transparenz und** Rechenschaftspflicht sicherzustellen.

Mehrheit der Agenturbediensteten sollte unmittelbar mit der operativen Umsetzung des Mandats der Agentur befasst sein. Dem Sitzmitgliedstaat und anderen Mitgliedstaaten sollte es erlaubt sein, freiwillige Beiträge zu den Einnahmen der Agentur zu leisten. Sämtliche Zuschüsse aus dem Gesamthaushaltsplan der Europäischen Union sollten dem Haushaltsverfahren der Union unterliegen. Ferner sollte die Rechnungsführung der Agentur durch den Rechnungshof geprüft werden, um **Transparenz, Rechenschaftspflicht, Effektivität und Zweckmäßigkeit der eingesetzten Mittel** sicherzustellen.

Or. cs

Änderungsantrag 82
Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung
Erwägung 47

Vorschlag der Kommission

(47) Die Konformitätsbewertung ist ein Verfahren, mit dem festgestellt wird, ob bestimmte Anforderungen an ein Produkt, einen Prozess, einen Dienst, ein System, eine Person oder ein Gremium erfüllt werden. Für die Zwecke dieser Verordnung ist unter **Zertifizierung** eine Art der Konformitätsbewertung zu verstehen, die sich auf die **Cybersicherheitsmerkmale** eines Produkts, eines Prozesses, eines Dienstes, eines Systems oder deren Kombination bezieht („IKT-Produkte und -Dienste“) und die von einem unabhängigen Dritten, bei dem es sich nicht um den Hersteller des Produkts oder den Diensteanbieter handelt, durchgeführt wird. Die Zertifizierung von IKT-Produkten und -Diensten an sich garantiert nicht, dass diese die Kriterien der Cybersicherheit

Geänderter Text

(47) Die Konformitätsbewertung ist ein Verfahren, mit dem festgestellt wird, ob bestimmte Anforderungen an ein Produkt, einen Prozess, einen Dienst, ein System, eine Person oder ein Gremium erfüllt werden. Für die Zwecke dieser Verordnung ist unter **Zertifizierung** eine Art der Konformitätsbewertung zu verstehen, die sich auf die **IT-Sicherheitsmerkmale** eines Produkts, eines Prozesses, eines Dienstes, eines Systems oder deren Kombination bezieht („IKT-Produkte und -Dienste“) und die von einem unabhängigen Dritten, bei dem es sich nicht um den Hersteller des Produkts oder den Diensteanbieter handelt, durchgeführt wird. **Während für die Zertifizierung bei Vertrauenswürdigkeitsstufen, die niedriger als „hoch“ eingestuft werden,**

erfüllen. Es handelt sich vielmehr um ein Verfahren und eine technische Methodik, um zu bescheinigen, dass die IKT-Produkte und -Dienste geprüft wurden und bestimmte, z. B. in technischen Normen festgelegte Anforderungen an die **Cybersicherheit** erfüllen.

eine Konformitätsbewertung ausreichend sein kann, sind für die Vertrauenswürdigkeitsstufe „hoch“ eine umfassende Sicherheitsbewertung und eine Zertifizierung durch eine neutrale Stelle erforderlich. Zertifikate dieser Vertrauenswürdigkeitsstufe sollten daher nur von den für Cybersicherheit zuständigen Aufsichtsbehörden ausgestellt werden. Die Ausstellung dieser Zertifikate sollte einer Begutachtung durch andere für Cybersicherheit zuständige Aufsichtsbehörden unterliegen. Die Zertifizierung von IKT-Produkten und -Diensten an sich garantiert nicht, dass diese die Kriterien der Cybersicherheit erfüllen. Es handelt sich vielmehr um ein Verfahren und eine technische Methodik, um zu bescheinigen, dass die IKT-Produkte und -Dienste geprüft wurden und bestimmte, z. B. in technischen Normen festgelegte Anforderungen an die **IT-Sicherheit** erfüllen.

Or. en

Änderungsantrag 83 **Roberta Metsola**

Vorschlag für eine Verordnung **Erwägung 47**

Vorschlag der Kommission

(47) Die Konformitätsbewertung ist ein Verfahren, mit dem festgestellt wird, ob bestimmte Anforderungen an ein Produkt, einen Prozess, einen Dienst, ein System, eine Person oder ein Gremium erfüllt werden. Für die Zwecke dieser Verordnung ist unter Zertifizierung eine Art der Konformitätsbewertung zu verstehen, die sich auf die Cybersicherheitsmerkmale eines Produkts, eines Prozesses, eines Dienstes, eines Systems oder deren Kombination bezieht (**„IKT-Produkte und**

Geänderter Text

(47) Die Konformitätsbewertung ist ein Verfahren, mit dem festgestellt wird, ob bestimmte Anforderungen an ein Produkt, einen Prozess, einen Dienst, ein System, eine Person oder ein Gremium erfüllt werden. Für die Zwecke dieser Verordnung ist unter Zertifizierung eine Art der Konformitätsbewertung zu verstehen, die sich auf die Cybersicherheitsmerkmale eines Produkts, eines Prozesses, eines Dienstes, eines Systems oder deren Kombination bezieht (**„IKT-Hardware-**

-Dienste“) und die von einem unabhängigen Dritten, **bei dem es sich nicht um den Hersteller des Produkts oder den Diensteanbieter handelt**, durchgeführt wird. Die Zertifizierung von IKT-Produkten und -Diensten an sich garantiert nicht, dass diese die Kriterien der Cybersicherheit erfüllen. Es handelt sich vielmehr um ein Verfahren und eine technische Methodik, um zu bescheinigen, dass die **IKT-Produkte und -Dienste** geprüft wurden und bestimmte, z. B. in technischen Normen festgelegte Anforderungen an die Cybersicherheit erfüllen.

und Software-Produkte und -Dienste“) und die von einem unabhängigen Dritten **oder im Rahmen eines strengen Verfahrens zur Konformitäts-Eigenerklärung gemäß Artikel 2 Absatz 1 Ziffer 16a, Artikel 46, Artikel 50 und Artikel 51 dieser Verordnung** durchgeführt wird. Die Zertifizierung von IKT-Produkten und -Diensten an sich garantiert nicht, dass diese die Kriterien der Cybersicherheit erfüllen. Es handelt sich vielmehr um ein Verfahren und eine technische Methodik, um zu bescheinigen, dass die **IKT-Hardware- und Software-Produkte und -Dienste** geprüft wurden und bestimmte, z. B. in technischen Normen festgelegte Anforderungen an die Cybersicherheit erfüllen.

Or. en

Änderungsantrag 84 **Anneleen Van Bossuyt, Daniel Dalton**

Vorschlag für eine Verordnung **Erwägung 47**

Vorschlag der Kommission

(47) Die Konformitätsbewertung ist ein Verfahren, mit dem festgestellt wird, ob bestimmte Anforderungen an ein Produkt, einen Prozess, einen Dienst, ein System, eine Person oder ein Gremium erfüllt werden. Für die Zwecke dieser Verordnung ist unter Zertifizierung eine Art der Konformitätsbewertung zu verstehen, die sich auf die Cybersicherheitsmerkmale eines Produkts, eines Prozesses, eines Dienstes, eines Systems oder deren Kombination bezieht („IKT-Produkte und -Dienste“) und die von einem unabhängigen Dritten, bei dem es sich nicht um den Hersteller des Produkts oder den Diensteanbieter handelt, durchgeführt wird. Die Zertifizierung von IKT-Produkten und -Diensten an sich garantiert nicht, dass

Geänderter Text

(47) Die Konformitätsbewertung ist ein Verfahren, mit dem festgestellt wird, ob bestimmte Anforderungen an ein Produkt, einen Prozess, einen Dienst, ein System, eine Person oder ein Gremium erfüllt werden. Für die Zwecke dieser Verordnung ist unter Zertifizierung eine Art der Konformitätsbewertung zu verstehen, die sich auf die Cybersicherheitsmerkmale **und Verfahren** eines Produkts, eines Prozesses, eines Dienstes, eines Systems oder deren Kombination bezieht („IKT-Produkte und -Dienste“) und die von einem unabhängigen Dritten, bei dem es sich nicht um den Hersteller des Produkts oder den Diensteanbieter handelt, durchgeführt wird. Die Zertifizierung von IKT-Produkten und -Diensten an sich garantiert nicht, dass

diese die Kriterien der Cybersicherheit erfüllen. Es handelt sich vielmehr um ein Verfahren und eine technische Methodik, um zu bescheinigen, dass die IKT-Produkte und -Dienste geprüft wurden und bestimmte, z. B. in technischen Normen festgelegte Anforderungen an die Cybersicherheit erfüllen.

diese die Kriterien der Cybersicherheit erfüllen. Es handelt sich vielmehr um ein Verfahren und eine technische Methodik, um zu bescheinigen, dass die IKT-Produkte und -Dienste **sowie die zugrundeliegenden Prozesse und Systeme** geprüft wurden und bestimmte, z. B. in technischen Normen festgelegte Anforderungen an die Cybersicherheit erfüllen.

Or. en

Änderungsantrag 85

Liisa Jaakonsaari, Christel Schaldemose, Lucy Anderson

Vorschlag für eine Verordnung

Erwägung 47

Vorschlag der Kommission

(47) Die Konformitätsbewertung ist ein Verfahren, mit dem festgestellt wird, ob bestimmte Anforderungen an ein Produkt, einen Prozess, einen Dienst, ein System, eine Person oder ein Gremium erfüllt werden. Für die Zwecke dieser Verordnung ist unter Zertifizierung eine Art der Konformitätsbewertung zu verstehen, die sich auf die Cybersicherheitsmerkmale eines Produkts, eines Prozesses, eines Dienstes, eines Systems oder deren Kombination bezieht („IKT-Produkte und -Dienste“) und die von einem unabhängigen Dritten, bei dem es sich nicht um den Hersteller des Produkts oder den Diensteanbieter handelt, durchgeführt wird. Die Zertifizierung von IKT-Produkten und -Diensten an sich garantiert nicht, dass diese die Kriterien der Cybersicherheit erfüllen. Es handelt sich vielmehr um ein Verfahren und eine technische Methodik, um zu bescheinigen, dass die IKT-Produkte und -Dienste geprüft wurden und bestimmte, z. B. in technischen Normen festgelegte Anforderungen an die

Geänderter Text

(47) Die Konformitätsbewertung ist ein Verfahren, mit dem festgestellt wird, ob bestimmte Anforderungen an ein Produkt, einen Prozess, einen Dienst, ein System, eine Person oder ein Gremium erfüllt werden. Für die Zwecke dieser Verordnung ist unter Zertifizierung eine Art der Konformitätsbewertung zu verstehen, die sich auf die Cybersicherheitsmerkmale eines Produkts, eines Prozesses, eines Dienstes, eines Systems oder deren Kombination bezieht („IKT-Produkte und -Dienste“) und die von einem unabhängigen Dritten, bei dem es sich nicht um den Hersteller des Produkts oder den Diensteanbieter handelt, durchgeführt wird. Die Zertifizierung von IKT-Produkten und -Diensten an sich garantiert nicht, dass diese die Kriterien der Cybersicherheit erfüllen, **und die Endnutzer sollten darauf aufmerksam gemacht werden**. Es handelt sich vielmehr um ein Verfahren und eine technische Methodik, um zu bescheinigen, dass die IKT-Produkte und -Dienste geprüft wurden und bestimmte, z. B. in technischen Normen festgelegte

Cybersicherheit erfüllen.

Anforderungen an die Cybersicherheit erfüllen.

Or. en

Änderungsantrag 86
Philippe Juvin

Vorschlag für eine Verordnung
Erwägung 48

Vorschlag der Kommission

(48) Die Cybersicherheitszertifizierung spielt eine **große** Rolle, wenn es darum geht, das Vertrauen in IKT-Produkte und -Dienste zu stärken und deren Sicherheit zu erhöhen. Die Entwicklung des digitalen Binnenmarkts und insbesondere der Datenwirtschaft und des Internets der Dinge kommt nur voran, wenn in der breiten Öffentlichkeit das Vertrauen vorhanden ist, dass diese Produkte und Dienste ein **gewisses** Maß an Cybersicherheit gewährleisten. Vernetzte und automatisierte Fahrzeuge, elektronische medizinische Geräte, die automatischen Steuerungssysteme der Industrie oder intelligente Netze sind, um nur einige Beispiele zu nennen, Sektoren, in denen die Zertifizierung bereits breiten Einsatz findet oder in naher Zukunft eingesetzt werden soll. Die unter die NIS-Richtlinie fallenden Sektoren sind zudem Sektoren, in denen die Cybersicherheitszertifizierung ein maßgeblicher Faktor ist.

Geänderter Text

(48) Die **europäische** Cybersicherheitszertifizierung spielt eine **essentielle** Rolle, wenn es darum geht, das Vertrauen in IKT-Produkte und -Dienste zu stärken und deren Sicherheit zu erhöhen. Die Entwicklung des digitalen Binnenmarkts und insbesondere der Datenwirtschaft und des Internets der Dinge kommt nur voran, wenn in der breiten Öffentlichkeit das Vertrauen vorhanden ist, dass diese Produkte und Dienste ein **hohes** Maß an Cybersicherheit gewährleisten. Vernetzte und automatisierte Fahrzeuge, elektronische medizinische Geräte, die automatischen Steuerungssysteme der Industrie oder intelligente Netze sind, um nur einige Beispiele zu nennen, Sektoren, in denen die Zertifizierung bereits breiten Einsatz findet oder in naher Zukunft eingesetzt werden soll. Die unter die NIS-Richtlinie fallenden Sektoren sind zudem Sektoren, in denen die Cybersicherheitszertifizierung ein maßgeblicher Faktor ist.

Or. fr

Änderungsantrag 87
Roberta Metsola

Vorschlag für eine Verordnung
Erwägung 49

(49) In ihrer Mitteilung aus dem Jahr 2016 „Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche“ unterstrich die Kommission die Notwendigkeit hochwertiger, erschwinglicher und interoperabler Produkte und Lösungen für die Cybersicherheit. Allerdings ist das Angebot an **IKT-Produkten und -diensten** im Binnenmarkt nach wie vor geografisch stark zersplittert. Das liegt daran, dass sich die Cybersicherheitsbranche in Europa überwiegend aufgrund der Nachfrage der nationalen Regierungen entwickelt hat. Zudem gehört der Mangel an interoperablen Lösungen (technischen Normen), Verfahrensweisen und EU-weiten Zertifizierungsmechanismen zu den Defiziten, die den Binnenmarkt im Bereich der Cybersicherheit beeinträchtigen. Dies macht es zum einen für europäische Unternehmen schwerer, im nationalen, europäischen und weltweiten Wettbewerb zu bestehen. Zum anderen verringert sich dadurch das Angebot an tragfähiger und einsetzbarer Cybersicherheitstechnik, auf die Privatpersonen und Unternehmen zugreifen könnten. Auch in der Halbzeitbewertung der Umsetzung der Strategie für den digitalen Binnenmarkt unterstrich die Kommission die Bedeutung sicherer vernetzter Produkte und Systeme und verwies darauf, dass die Schaffung eines europäischen Rahmens für die IKT-Sicherheit, auf dessen Grundlage Vorschriften für die Organisation der IKT-Sicherheitszertifizierung in der Union festgelegt werden, dafür sorgen kann, dass das Vertrauen in den Binnenmarkt erhalten bleibt und die derzeitige Fragmentierung des Cybersicherheitsmarkts eingedämmt wird.

(49) In ihrer Mitteilung aus dem Jahr 2016 „Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche“ unterstrich die Kommission die Notwendigkeit hochwertiger, erschwinglicher und interoperabler Produkte und Lösungen für die Cybersicherheit. Allerdings ist das Angebot an **IKT-Hardware- und Software-Produkten und -Diensten** im Binnenmarkt nach wie vor geografisch stark zersplittert. Das liegt daran, dass sich die Cybersicherheitsbranche in Europa überwiegend aufgrund der Nachfrage der nationalen Regierungen entwickelt hat. Zudem gehört der Mangel an interoperablen Lösungen (technischen Normen), Verfahrensweisen und EU-weiten Zertifizierungsmechanismen zu den Defiziten, die den Binnenmarkt im Bereich der Cybersicherheit beeinträchtigen. Dies macht es zum einen für europäische Unternehmen schwerer, im nationalen, europäischen und weltweiten Wettbewerb zu bestehen. Zum anderen verringert sich dadurch das Angebot an tragfähiger und einsetzbarer Cybersicherheitstechnik, auf die Privatpersonen und Unternehmen zugreifen könnten. Auch in der Halbzeitbewertung der Umsetzung der Strategie für den digitalen Binnenmarkt unterstrich die Kommission die Bedeutung sicherer vernetzter Produkte und Systeme und verwies darauf, dass die Schaffung eines europäischen Rahmens für die IKT-Sicherheit, auf dessen Grundlage Vorschriften für die Organisation der IKT-Sicherheitszertifizierung in der Union festgelegt werden, dafür sorgen kann, dass das Vertrauen in den Binnenmarkt erhalten bleibt und die derzeitige Fragmentierung des Cybersicherheitsmarkts eingedämmt wird.

Änderungsantrag 88
Maria Grapini

Vorschlag für eine Verordnung
Erwägung 50

Vorschlag der Kommission

(50) Derzeit ist die Lage hinsichtlich der Cybersicherheitszertifizierung von IKT-Produkten und -Diensten in der EU sehr uneinheitlich. Wenn dies doch der Fall ist, geschieht es meist auf Ebene der Mitgliedstaaten oder im Rahmen brancheneigener Programme. So wird ein von einer nationalen Cybersicherheitsbehörde ausgestelltes Zertifikat nicht grundsätzlich auch von anderen Mitgliedstaaten anerkannt. Unternehmen müssen somit ihre Produkte und Dienste möglicherweise in mehreren Mitgliedstaaten, in denen sie tätig sind, zertifizieren lassen, um beispielsweise an einer nationalen Ausschreibung teilzunehmen. Auch wenn immer neue Systeme entstehen, scheint es kein kohärentes und ganzheitliches Konzept zu geben, das sich mit horizontalen Fragen der Cybersicherheit, etwa im Bereich des Internets der Dinge, befasst. Die vorhandenen Systeme weisen im Hinblick auf Produkterfassung, Vertrauenswürdigkeitsstufen, wesentliche Kriterien und tatsächliche Nutzung erhebliche Mängel und Unterschiede auf.

Geänderter Text

(50) Derzeit ist die Lage hinsichtlich der Cybersicherheitszertifizierung von IKT-Produkten und -Diensten in der EU sehr uneinheitlich. Wenn dies doch der Fall ist, geschieht es meist auf Ebene der Mitgliedstaaten oder im Rahmen brancheneigener Programme. So wird ein von einer nationalen Cybersicherheitsbehörde ausgestelltes Zertifikat nicht grundsätzlich auch von anderen Mitgliedstaaten anerkannt. Unternehmen müssen somit ihre Produkte und Dienste möglicherweise in mehreren Mitgliedstaaten, in denen sie tätig sind, zertifizieren lassen, um beispielsweise an einer nationalen Ausschreibung teilzunehmen, **wobei diese Ausschreibungen die Unternehmen finanziell zusätzlich belasten**. Auch wenn immer neue Systeme entstehen, scheint es kein kohärentes und ganzheitliches Konzept zu geben, das sich mit horizontalen Fragen der Cybersicherheit, etwa im Bereich des Internets der Dinge, befasst. Die vorhandenen Systeme weisen im Hinblick auf Produkterfassung, Vertrauenswürdigkeitsstufen, wesentliche Kriterien und tatsächliche Nutzung erhebliche Mängel und Unterschiede auf.

Or. ro

Änderungsantrag 89
Roberta Metsola

Vorschlag für eine Verordnung Erwägung 50

Vorschlag der Kommission

(50) Derzeit werden IKT-Produkte und -Dienste im Hinblick auf ihre Cybersicherheit kaum zertifiziert, und wenn doch, geschieht dies meist auf Ebene der Mitgliedstaaten oder im Rahmen brancheneigener Programme. So wird ein von einer nationalen Cybersicherheitsbehörde ausgestelltes Zertifikat nicht grundsätzlich auch von anderen Mitgliedstaaten anerkannt. Unternehmen müssen somit ihre Produkte und Dienste möglicherweise in mehreren Mitgliedstaaten, in denen sie tätig sind, zertifizieren lassen, um beispielsweise an einer nationalen Ausschreibung teilzunehmen. Auch wenn immer neue Systeme entstehen, scheint es kein kohärentes und ganzheitliches Konzept zu geben, das sich mit horizontalen Fragen der Cybersicherheit, etwa im Bereich des Internets der Dinge, befasst. Die vorhandenen Systeme weisen im Hinblick auf Produkterfassung, Vertrauenswürdigkeitsstufen, wesentliche Kriterien und tatsächliche Nutzung erhebliche Mängel und Unterschiede auf.

Geänderter Text

(50) Derzeit werden IKT-Produkte und -Dienste im Hinblick auf ihre Cybersicherheit kaum zertifiziert, und wenn doch, geschieht dies meist auf Ebene der Mitgliedstaaten oder im Rahmen brancheneigener Programme. So wird ein von einer nationalen Cybersicherheitsbehörde ausgestelltes Zertifikat nicht grundsätzlich auch von anderen Mitgliedstaaten anerkannt. Unternehmen müssen somit ihre Produkte und Dienste möglicherweise in mehreren Mitgliedstaaten, in denen sie tätig sind, zertifizieren lassen, um beispielsweise an einer nationalen Ausschreibung teilzunehmen. Auch wenn immer neue Systeme entstehen, scheint es kein kohärentes und ganzheitliches Konzept zu geben, das sich mit horizontalen Fragen der Cybersicherheit, etwa im Bereich des Internets der Dinge, befasst. Die vorhandenen Systeme weisen im Hinblick auf Produkterfassung, *risikobasierte* Vertrauenswürdigkeitsstufen, wesentliche Kriterien und tatsächliche Nutzung erhebliche Mängel und Unterschiede auf.

Or. en

Änderungsantrag 90
Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung Erwägung 52

Vorschlag der Kommission

(52) Vor diesem Hintergrund gilt es, einen europäischen Rahmen für die **Cybersicherheitszertifizierung** aufzubauen, auf dessen Grundlage die

Geänderter Text

(52) Vor diesem Hintergrund gilt es, einen europäischen Rahmen für die **IT-Sicherheitszertifizierung** aufzubauen, auf dessen Grundlage die Anforderungen an

Anforderungen an die zu entwickelnden europäischen Systeme zur Zertifizierung der **Cybersicherheit** festgelegt werden, damit die Zertifikate für die IKT-Produkte und -Dienste in allen Mitgliedstaaten anerkannt und verwendet werden können. Mit einem europäischen Rahmen werden zwei Ziele verfolgt: einerseits dürfte er dazu beitragen, das Vertrauen in IKT-Produkte und -Dienste zu erhöhen, die nach solchen Systemen zertifiziert wurden, und andererseits dürften sich so vielfältige, sich widersprechende oder überlappende nationale System für die **Cybersicherheitszertifizierung** vermeiden lassen, was die Kosten für auf dem digitalen Binnenmarkt tätige Unternehmen senkt. Die Systeme sollten nichtdiskriminierend sein und sich auf internationale bzw. europäische Normen stützen, sofern diese Normen nicht unwirksam oder unangemessen im Hinblick auf die Erreichung der legitimen Ziele der EU in diesem Bereich sind.

die zu entwickelnden europäischen Systeme zur Zertifizierung der **IT-Sicherheit** festgelegt werden, damit die Zertifikate für die IKT-Produkte und -Dienste in allen Mitgliedstaaten anerkannt und verwendet werden können. Mit einem europäischen Rahmen werden zwei Ziele verfolgt: einerseits dürfte er dazu beitragen, das Vertrauen in IKT-Produkte und -Dienste zu erhöhen, die nach solchen Systemen zertifiziert wurden, und andererseits dürften sich so vielfältige, sich widersprechende oder überlappende nationale System für die **IT-Sicherheitszertifizierung** vermeiden lassen, was die Kosten für auf dem digitalen Binnenmarkt tätige Unternehmen senkt. Diese Systeme sollten **sich an dem Prinzip der eingebauten Sicherheit und an den in Verordnung (EU) 2016/679 genannten Grundsätzen orientieren. Außerdem sollten sie** nichtdiskriminierend sein und sich auf internationale bzw. europäische Normen stützen, sofern diese Normen nicht unwirksam oder unangemessen im Hinblick auf die Erreichung der legitimen Ziele der EU in diesem Bereich sind.

Or. en

Begründung

Einführung der Grundprinzipien für die Zertifizierungssysteme

Änderungsantrag 91 **Roberta Metsola**

Vorschlag für eine Verordnung **Erwägung 52**

Vorschlag der Kommission

(52) Vor diesem Hintergrund gilt es, einen europäischen Rahmen für die Cybersicherheitszertifizierung aufzubauen, auf dessen Grundlage die Anforderungen

Geänderter Text

(52) Vor diesem Hintergrund gilt es, einen europäischen Rahmen für die Cybersicherheitszertifizierung aufzubauen, auf dessen Grundlage die Anforderungen

an die zu entwickelnden europäischen Systeme zur Zertifizierung der Cybersicherheit festgelegt werden, damit die Zertifikate für die **IKT-Produkte und -Dienste** in allen Mitgliedstaaten anerkannt und verwendet werden können. Mit einem europäischen Rahmen werden zwei Ziele verfolgt: einerseits dürfte er dazu beitragen, das Vertrauen in **IKT-Produkte und -Dienste** zu erhöhen, die nach solchen Systemen zertifiziert wurden, und andererseits dürften sich so vielfältige, sich widersprechende oder überlappende nationale System für die Cybersicherheitszertifizierung vermeiden lassen, was die Kosten für auf dem digitalen Binnenmarkt tätige Unternehmen senkt. Die Systeme sollten nichtdiskriminierend sein und sich auf internationale bzw. europäische Normen stützen, sofern diese Normen nicht unwirksam oder unangemessen im Hinblick auf die Erreichung der legitimen Ziele der EU in diesem Bereich sind.

an die zu entwickelnden europäischen Systeme zur Zertifizierung der Cybersicherheit festgelegt werden, damit die Zertifikate für die **IKT-Hardware- und Software-Produkte und -Dienste** in allen Mitgliedstaaten anerkannt und verwendet werden können. Mit einem europäischen Rahmen werden zwei Ziele verfolgt: einerseits dürfte er dazu beitragen, das Vertrauen in **IKT-Hardware- und Software-Produkte und -Dienste** zu erhöhen, die nach solchen Systemen zertifiziert wurden, und andererseits dürften sich so vielfältige, sich widersprechende oder überlappende nationale System für die Cybersicherheitszertifizierung vermeiden lassen, was die Kosten für auf dem digitalen Binnenmarkt tätige Unternehmen senkt. Die Systeme sollten nichtdiskriminierend sein und sich auf internationale bzw. europäische Normen stützen, sofern diese Normen nicht unwirksam oder unangemessen im Hinblick auf die Erreichung der legitimen Ziele der EU in diesem Bereich sind.

Or. en

Änderungsantrag 92 **Philippe Juvin**

Vorschlag für eine Verordnung **Erwägung 52**

Vorschlag der Kommission

(52) Vor diesem Hintergrund gilt es, einen europäischen Rahmen für die Cybersicherheitszertifizierung aufzubauen, auf dessen Grundlage die Anforderungen an die zu entwickelnden europäischen Systeme zur Zertifizierung der Cybersicherheit festgelegt werden, damit die Zertifikate für die IKT-Produkte und -Dienste in allen Mitgliedstaaten anerkannt und verwendet werden können. Mit einem

Geänderter Text

(52) Vor diesem Hintergrund gilt es, **einen gemeinsamen Ansatz zu verfolgen und** einen europäischen Rahmen für die Cybersicherheitszertifizierung aufzubauen, auf dessen Grundlage die Anforderungen an die zu entwickelnden europäischen Systeme zur Zertifizierung der Cybersicherheit festgelegt werden, damit die Zertifikate für die IKT-Produkte und -Dienste in allen Mitgliedstaaten anerkannt

europäischen Rahmen werden zwei Ziele verfolgt: einerseits dürfte er dazu beitragen, das Vertrauen in IKT-Produkte und -Dienste zu erhöhen, die nach solchen Systemen zertifiziert wurden, und andererseits dürften sich so vielfältige, sich widersprechende oder überlappende nationale System für die Cybersicherheitszertifizierung vermeiden lassen, was die Kosten für auf dem digitalen Binnenmarkt tätige Unternehmen senkt. Die Systeme sollten nichtdiskriminierend sein und sich auf internationale bzw. europäische Normen stützen, sofern diese Normen nicht unwirksam oder unangemessen im Hinblick auf die Erreichung der legitimen Ziele der EU in diesem Bereich sind.

und verwendet werden können. Mit einem europäischen Rahmen werden zwei Ziele verfolgt: einerseits dürfte er dazu beitragen, das Vertrauen in IKT-Produkte und -Dienste zu erhöhen, die nach solchen Systemen zertifiziert wurden, und andererseits dürften sich so vielfältige, sich widersprechende oder überlappende nationale System für die Cybersicherheitszertifizierung vermeiden lassen, was die Kosten für auf dem digitalen Binnenmarkt tätige Unternehmen senkt. Die Systeme sollten nichtdiskriminierend sein und sich auf internationale bzw. europäische Normen stützen, sofern diese Normen nicht unwirksam oder unangemessen im Hinblick auf die Erreichung der legitimen Ziele der EU in diesem Bereich sind.

Or. fr

Änderungsantrag 93
Philippe Juvin, Andreas Schwab

Vorschlag für eine Verordnung
Erwägung 52 a (neu)

Vorschlag der Kommission

Geänderter Text

(52a) Dieser europäische Rahmen für die Cybersicherheitszertifizierung muss in homogener Weise in allen Mitgliedstaaten eingeführt werden, um zu vermeiden, dass es aufgrund von unterschiedlich hohen Kosten oder Anforderungsniveaus zwischen den Mitgliedstaaten zu einem „Zertifikate-Shopping“ kommt.

Or. fr

Änderungsantrag 94
Roberta Metsola

Vorschlag für eine Verordnung

Erwägung 53

Vorschlag der Kommission

(53) Die Kommission sollte befugt sein, für bestimmte Gruppen von **IKT-Produkten und -Diensten** europäische Systeme für die Cybersicherheitszertifizierung anzunehmen. Diese Systeme sollten von nationalen Aufsichtsbehörden für die Zertifizierung umgesetzt und überwacht werden, und die im Rahmen dieser Systeme erteilten Zertifikate sollten unionsweit gültig sein und anerkannt werden. Die von der Industrie oder sonstigen privaten Organisationen betriebenen Zertifizierungssysteme fallen nicht in den Anwendungsbereich dieser Verordnung. Die Stellen, die solche Systeme betreiben, können der Kommission jedoch vorschlagen, ihre Systeme als Grundlage für ein europäisches System in Betracht zu ziehen und sie als ein solches zu genehmigen.

Geänderter Text

(53) Die Kommission sollte befugt sein, für bestimmte Gruppen von **IKT-Hardware- und Software-Produkten und -Diensten** europäische Systeme für die Cybersicherheitszertifizierung anzunehmen. Diese Systeme sollten von nationalen Aufsichtsbehörden für die Zertifizierung umgesetzt und überwacht werden, und die im Rahmen dieser Systeme erteilten Zertifikate sollten unionsweit gültig sein und anerkannt werden. Die von der Industrie oder sonstigen privaten Organisationen betriebenen Zertifizierungssysteme fallen nicht in den Anwendungsbereich dieser Verordnung. Die Stellen, die solche Systeme betreiben, können der Kommission jedoch vorschlagen, ihre Systeme als Grundlage für ein europäisches System in Betracht zu ziehen und sie als ein solches zu genehmigen.

Or. en

Änderungsantrag 95 Mylène Troszczynski

Vorschlag für eine Verordnung Erwägung 53

Vorschlag der Kommission

(53) **Die** Kommission **sollte befugt sein**, für bestimmte Gruppen von IKT-Produkten und -Diensten **europäische Systeme für die Cybersicherheitszertifizierung anzunehmen**. Diese Systeme sollten von nationalen Aufsichtsbehörden für die Zertifizierung umgesetzt und überwacht werden, und die im Rahmen dieser Systeme erteilten Zertifikate sollten unionsweit gültig sein und anerkannt werden. Die von der Industrie oder

Geänderter Text

(53) **Die Mitgliedstaaten setzen die Kommission von ihren Entscheidungen zu europäischen Systemen für die Cybersicherheitszertifizierung** für bestimmte Gruppen von IKT-Produkten und -Diensten **in Kenntnis**. Diese Systeme sollten von nationalen Aufsichtsbehörden für die Zertifizierung umgesetzt und überwacht werden, und die im Rahmen dieser Systeme erteilten Zertifikate sollten unionsweit gültig sein und anerkannt

sonstigen privaten Organisationen betriebenen Zertifizierungssysteme fallen nicht in den Anwendungsbereich dieser Verordnung. Die Stellen, die solche Systeme betreiben, können der Kommission jedoch vorschlagen, ihre Systeme als Grundlage für ein europäisches System in Betracht zu ziehen und sie als ein solches zu genehmigen.

werden. Die von der Industrie oder sonstigen privaten Organisationen betriebenen Zertifizierungssysteme fallen nicht in den Anwendungsbereich dieser Verordnung. Die Stellen, die solche Systeme betreiben, können der Kommission jedoch vorschlagen, ihre Systeme als Grundlage für ein europäisches System in Betracht zu ziehen und sie als ein solches zu genehmigen.

Or. fr

Änderungsantrag 96
Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Erwägung 55

Vorschlag der Kommission

(55) Mit den europäischen Systemen für die Cybersicherheitszertifizierung sollte gewährleistet werden, dass die nach solchen Systemen zertifizierten IKT-Produkte und -Dienste bestimmten Anforderungen genügen. Diese Anforderungen beziehen sich auf die Fähigkeit, auf einer bestimmten Vertrauenswürdigkeitsstufe Handlungen zu widerstehen, die darauf abzielen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten, Funktionen oder Dienste zu beeinträchtigen, die von diesen Produkten, Prozessen, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden. In dieser Verordnung können nicht alle Anforderungen an die Cybersicherheit sämtlicher IKT-Produkte und -Dienste im Einzelnen festgelegt werden. Die Vielfalt der IKT-Produkte und -Dienste und die damit zusammenhängenden Anforderungen an die Cybersicherheit ist so groß, dass es sehr schwierig ist, allgemeine Anforderungen

Geänderter Text

(55) Mit den europäischen Systemen für die Cybersicherheitszertifizierung sollte gewährleistet werden, dass die nach solchen Systemen zertifizierten IKT-Produkte und -Dienste bestimmten Anforderungen genügen. Diese Anforderungen beziehen sich auf die Fähigkeit, auf einer bestimmten Vertrauenswürdigkeitsstufe Handlungen zu widerstehen, die darauf abzielen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten, Funktionen oder Dienste zu beeinträchtigen, die von diesen Produkten, Prozessen, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden. In dieser Verordnung können nicht alle Anforderungen an die Cybersicherheit sämtlicher IKT-Produkte und -Dienste im Einzelnen festgelegt werden. Die Vielfalt der IKT-Produkte und -Dienste und die damit zusammenhängenden Anforderungen an die Cybersicherheit ist so groß, dass es sehr schwierig ist, allgemeine Anforderungen

an die Cybersicherheit für alle Eventualitäten festzulegen. Es gilt daher, ein breit gefasstes und allgemeines Konzept der Cybersicherheit für die Zwecke der Zertifizierung zu verabschieden, ergänzt durch besondere Cybersicherheitsziele, die bei der Konzeption der europäischen Systeme für die Cybersicherheitszertifizierung berücksichtigt werden müssen. Die Modalitäten, wie diese Ziele für bestimmte IKT-Produkte und -Dienste erreicht werden, sollten dann weiter im Einzelnen auf der Grundlage des jeweiligen von der Kommission angenommenen Zertifizierungssystems festgelegt werden, etwa durch Verweise auf Normen oder technische Spezifikationen.

an die Cybersicherheit für alle Eventualitäten festzulegen. Es gilt daher, ein breit gefasstes und allgemeines Konzept der Cybersicherheit für die Zwecke der Zertifizierung zu verabschieden, ergänzt durch besondere Cybersicherheitsziele, die bei der Konzeption der europäischen Systeme für die Cybersicherheitszertifizierung berücksichtigt werden müssen. Die Modalitäten, wie diese Ziele für bestimmte IKT-Produkte und -Dienste erreicht werden, sollten dann weiter im Einzelnen auf der Grundlage des jeweiligen von der Kommission angenommenen Zertifizierungssystems festgelegt werden, etwa durch Verweise auf Normen oder technische Spezifikationen. ***Von entscheidender Bedeutung ist, dass jedes europäische System zur Zertifizierung der Cybersicherheit derart gestaltet werden sollte, dass es alle betreffenden in den Sektor involvierten Akteure anregt und ermuntert, Sicherheitsstandards, technische Normen und die Grundsätze der eingebauten Sicherheit in allen Phasen des Lebenszyklus von Produkten oder Diensten zu entwickeln und umzusetzen.***

Or. en

Änderungsantrag 97 **Roberta Metsola**

Vorschlag für eine Verordnung **Erwägung 55**

Vorschlag der Kommission

(55) Mit den europäischen Systemen für die Cybersicherheitszertifizierung sollte gewährleistet werden, dass die nach solchen Systemen zertifizierten ***IKT-Produkte und -Dienste*** bestimmten Anforderungen genügen. Diese Anforderungen beziehen sich auf die

Geänderter Text

(55) Mit den europäischen Systemen für die Cybersicherheitszertifizierung sollte gewährleistet werden, dass die nach solchen Systemen zertifizierten ***IKT-Hardware- und Software-Produkte und -Dienste*** bestimmten Anforderungen genügen. Diese Anforderungen beziehen

Fähigkeit, auf einer bestimmten Vertrauenswürdigkeitsstufe Handlungen zu widerstehen, die darauf abzielen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten, Funktionen oder Dienste zu beeinträchtigen, die von diesen Produkten, Prozessen, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden. In dieser Verordnung können nicht alle Anforderungen an die Cybersicherheit sämtlicher **IKT-Produkte und -Dienste** im Einzelnen festgelegt werden. Die Vielfalt der **IKT-Produkte und -Dienste** und die damit zusammenhängenden Anforderungen an die Cybersicherheit ist so groß, dass es sehr schwierig ist, allgemeine Anforderungen an die Cybersicherheit für alle Eventualitäten festzulegen. Es gilt daher, ein breit gefasstes und allgemeines Konzept der Cybersicherheit für die Zwecke der Zertifizierung zu verabschieden, ergänzt durch besondere Cybersicherheitsziele, die bei der Konzeption der europäischen Systeme für die Cybersicherheitszertifizierung berücksichtigt werden müssen. Die Modalitäten, wie diese Ziele für bestimmte **IKT-Produkte und -Dienste** erreicht werden, sollten dann weiter im Einzelnen auf der Grundlage des jeweiligen von der Kommission angenommenen Zertifizierungssystems festgelegt werden, etwa durch Verweise auf Normen oder technische Spezifikationen.

sich auf die Fähigkeit, auf einer bestimmten Vertrauenswürdigkeitsstufe Handlungen zu widerstehen, die darauf abzielen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten, Funktionen oder Dienste zu beeinträchtigen, die von diesen Produkten, Prozessen, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden. In dieser Verordnung können nicht alle Anforderungen an die Cybersicherheit sämtlicher **IKT-Hardware- und Software-Produkte und -Dienste** im Einzelnen festgelegt werden. Die Vielfalt der **IKT-Hardware- und Software-Produkte und -Dienste** und die damit zusammenhängenden Anforderungen an die Cybersicherheit ist so groß, dass es sehr schwierig ist, allgemeine Anforderungen an die Cybersicherheit für alle Eventualitäten festzulegen. Es gilt daher, ein breit gefasstes und allgemeines Konzept der Cybersicherheit für die Zwecke der Zertifizierung zu verabschieden, ergänzt durch besondere Cybersicherheitsziele, die bei der Konzeption der europäischen Systeme für die Cybersicherheitszertifizierung berücksichtigt werden müssen. **Dazu sollte eine Checkliste verwendet werden, in der die Risiken aufgeführt sind, denen die IKT-Hardware- und Software-Produkte und -Dienste bei einer bestimmten Kategorie von Nutzern und in einem bestimmten Umfeld voraussichtlich ausgesetzt sein werden.** Die Modalitäten, wie diese Ziele für bestimmte **IKT-Hardware- und Software-Produkte und -Dienste** erreicht werden, sollten dann weiter im Einzelnen auf der Grundlage des jeweiligen von der Kommission angenommenen Zertifizierungssystems festgelegt werden, etwa durch Verweise auf Normen oder technische Spezifikationen.

Or. en

Änderungsantrag 98

Liisa Jaakonsaari, Christel Schaldemose, Lucy Anderson

Vorschlag für eine Verordnung

Erwägung 55

Vorschlag der Kommission

(55) Mit den europäischen Systemen für die Cybersicherheitszertifizierung sollte gewährleistet werden, dass die nach solchen Systemen zertifizierten IKT-Produkte und -Dienste bestimmten Anforderungen genügen. Diese Anforderungen beziehen sich auf die Fähigkeit, auf einer bestimmten Vertrauenswürdigkeitsstufe Handlungen zu widerstehen, die darauf abzielen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten, Funktionen oder Dienste zu beeinträchtigen, die von diesen Produkten, Prozessen, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden. In dieser Verordnung können nicht alle Anforderungen an die Cybersicherheit sämtlicher IKT-Produkte und -Dienste im Einzelnen festgelegt werden. Die Vielfalt der IKT-Produkte und -Dienste und die damit zusammenhängenden Anforderungen an die Cybersicherheit ist so groß, dass es sehr schwierig ist, allgemeine Anforderungen an die Cybersicherheit für alle Eventualitäten festzulegen. Es gilt daher, ein breit gefasstes und allgemeines Konzept der Cybersicherheit für die Zwecke der Zertifizierung zu verabschieden, ergänzt durch besondere Cybersicherheitsziele, die bei der Konzeption der europäischen Systeme für die Cybersicherheitszertifizierung berücksichtigt werden müssen. Die Modalitäten, wie diese Ziele für bestimmte IKT-Produkte und -Dienste erreicht werden, sollten dann weiter im Einzelnen

Geänderter Text

(55) Mit den europäischen Systemen für die Cybersicherheitszertifizierung sollte gewährleistet werden, dass die nach solchen Systemen zertifizierten IKT-Produkte und -Dienste bestimmten Anforderungen genügen. Diese Anforderungen beziehen sich auf die Fähigkeit, auf einer bestimmten Vertrauenswürdigkeitsstufe Handlungen zu widerstehen, die darauf abzielen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten, Funktionen oder Dienste zu beeinträchtigen, die von diesen Produkten, Prozessen, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden. In dieser Verordnung können nicht alle Anforderungen an die Cybersicherheit sämtlicher IKT-Produkte und -Dienste im Einzelnen festgelegt werden. Die Vielfalt der IKT-Produkte und -Dienste und die damit zusammenhängenden Anforderungen an die Cybersicherheit ist so groß, dass es sehr schwierig ist, allgemeine Anforderungen an die Cybersicherheit für alle Eventualitäten festzulegen. Es gilt daher, ein breit gefasstes und allgemeines Konzept der Cybersicherheit für die Zwecke der Zertifizierung zu verabschieden, ergänzt durch besondere Cybersicherheitsziele, die bei der Konzeption der europäischen Systeme für die Cybersicherheitszertifizierung berücksichtigt werden müssen. Die Modalitäten, wie diese Ziele für bestimmte IKT-Produkte und -Dienste erreicht werden, sollten dann weiter im Einzelnen

auf der Grundlage des jeweiligen von der Kommission angenommenen Zertifizierungssystems festgelegt werden, etwa durch Verweise auf Normen oder technische Spezifikationen.

auf der Grundlage des jeweiligen von der Kommission angenommenen Zertifizierungssystems festgelegt werden, etwa durch Verweise auf Normen oder technische Spezifikationen. ***Wenn das Zertifizierungssystem Siegel oder Kennzeichen vorsieht, sind die Bedingungen für die Verwendung dieser Siegel bzw. Kennzeichen darzulegen. Die Siegel und Kennzeichen müssen für die Endnutzer klar und leicht verständlich sein.***

Or. en

Änderungsantrag 99 **Dennis de Jong**

Vorschlag für eine Verordnung **Erwägung 55**

Vorschlag der Kommission

(55) Mit den europäischen Systemen für die Cybersicherheitszertifizierung sollte gewährleistet werden, dass die nach solchen Systemen zertifizierten IKT-Produkte und -Dienste bestimmten Anforderungen genügen. Diese Anforderungen beziehen sich auf die Fähigkeit, auf einer bestimmten Vertrauenswürdigkeitsstufe Handlungen zu widerstehen, die darauf abzielen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten, Funktionen oder Dienste zu beeinträchtigen, die von diesen Produkten, Prozessen, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden. In dieser Verordnung können nicht alle Anforderungen an die Cybersicherheit sämtlicher IKT-Produkte und -Dienste im Einzelnen festgelegt werden. Die Vielfalt der IKT-Produkte und -Dienste und die damit zusammenhängenden Anforderungen an

Geänderter Text

(55) Mit den europäischen Systemen für die Cybersicherheitszertifizierung sollte gewährleistet werden, dass die nach solchen Systemen zertifizierten IKT-Produkte und -Dienste bestimmten Anforderungen genügen. Diese Anforderungen beziehen sich auf die Fähigkeit, auf einer bestimmten Vertrauenswürdigkeitsstufe Handlungen zu widerstehen, die darauf abzielen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten, Funktionen oder Dienste zu beeinträchtigen, die von diesen Produkten, Prozessen, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden. In dieser Verordnung können nicht alle Anforderungen an die Cybersicherheit sämtlicher IKT-Produkte und -Dienste im Einzelnen festgelegt werden. Die Vielfalt der IKT-Produkte und -Dienste und die damit zusammenhängenden Anforderungen an

die Cybersicherheit ist so groß, dass es sehr schwierig ist, allgemeine Anforderungen an die Cybersicherheit für alle Eventualitäten festzulegen. Es gilt daher, ein breit gefasstes und allgemeines Konzept der Cybersicherheit für die Zwecke der Zertifizierung zu verabschieden, ergänzt durch besondere Cybersicherheitsziele, die bei der Konzeption der europäischen Systeme für die Cybersicherheitszertifizierung berücksichtigt werden müssen. Die Modalitäten, wie diese Ziele für bestimmte IKT-Produkte und -Dienste erreicht werden, sollten dann weiter im Einzelnen auf der Grundlage des jeweiligen von der Kommission angenommenen Zertifizierungssystems festgelegt werden, etwa durch Verweise auf Normen oder technische Spezifikationen.

die Cybersicherheit ist so groß, dass es sehr schwierig ist, allgemeine Anforderungen an die Cybersicherheit für alle Eventualitäten festzulegen. Es gilt daher, ein breit gefasstes und allgemeines Konzept der Cybersicherheit für die Zwecke der Zertifizierung zu verabschieden, ergänzt durch besondere Cybersicherheitsziele, die bei der Konzeption der europäischen Systeme für die Cybersicherheitszertifizierung berücksichtigt werden müssen. Die Modalitäten, wie diese Ziele für bestimmte IKT-Produkte und -Dienste erreicht werden, sollten dann weiter im Einzelnen auf der Grundlage des jeweiligen von der Kommission angenommenen Zertifizierungssystems festgelegt werden, etwa durch Verweise auf Normen oder technische Spezifikationen. ***In Abhängigkeit vom jeweiligen Zertifizierungssystem könnte prinzipiell der Rückgriff auf vorhandene bewährte Verfahren bei der Festlegung bestimmter Anforderungen des Systems in Frage kommen.***

Or. en

Begründung

Im Bereich IKT gibt es bereits viele bewährte Verfahren, die in Sicherheits-Fachkreisen akzeptiert sind und (fast) alle Schwachstellen abdecken. Ein neues System könnte daher auf dem bereits vorhandenen Wissen aufbauen. Wenn es im Interesse der EU liegt, diese bewährten Verfahren zu ändern, dann sollte dies leicht zu begründen sein.

Änderungsantrag 100 Lambert van Nistelrooij

Vorschlag für eine Verordnung Erwägung 55

Vorschlag der Kommission

(55) Mit den europäischen Systemen für die Cybersicherheitszertifizierung sollte gewährleistet werden, dass die nach

Geänderter Text

(55) Mit den europäischen Systemen für die Cybersicherheitszertifizierung sollte gewährleistet werden, dass die nach

solchen Systemen zertifizierten IKT-Produkte und -Dienste bestimmten Anforderungen genügen. Diese Anforderungen beziehen sich auf die Fähigkeit, auf einer bestimmten Vertrauenswürdigkeitsstufe Handlungen zu widerstehen, die darauf abzielen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten, Funktionen oder Dienste zu beeinträchtigen, die von diesen Produkten, Prozessen, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden. In dieser Verordnung können nicht alle Anforderungen an die Cybersicherheit sämtlicher IKT-Produkte und -Dienste im Einzelnen festgelegt werden. Die Vielfalt der IKT-Produkte und -Dienste und die damit zusammenhängenden Anforderungen an die Cybersicherheit ist so groß, dass es sehr schwierig ist, allgemeine Anforderungen an die Cybersicherheit für alle Eventualitäten festzulegen. Es gilt daher, ein breit gefasstes und allgemeines Konzept der Cybersicherheit für die Zwecke der Zertifizierung zu verabschieden, ergänzt durch besondere Cybersicherheitsziele, die bei der Konzeption der europäischen Systeme für die Cybersicherheitszertifizierung berücksichtigt werden müssen. Die Modalitäten, wie diese Ziele für bestimmte IKT-Produkte und -Dienste erreicht werden, sollten dann weiter im Einzelnen auf der Grundlage des jeweiligen von der Kommission angenommenen Zertifizierungssystems festgelegt werden, etwa durch Verweise auf Normen oder technische Spezifikationen.

solchen Systemen zertifizierten IKT-Produkte und -Dienste bestimmten Anforderungen genügen. Diese Anforderungen beziehen sich auf die Fähigkeit, auf einer bestimmten Vertrauenswürdigkeitsstufe Handlungen zu widerstehen, die darauf abzielen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten, Funktionen oder Dienste zu beeinträchtigen, die von diesen Produkten, Prozessen, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden. In dieser Verordnung können nicht alle Anforderungen an die Cybersicherheit sämtlicher IKT-Produkte und -Dienste im Einzelnen festgelegt werden. Die Vielfalt der IKT-Produkte und -Dienste und die damit zusammenhängenden Anforderungen an die Cybersicherheit ist so groß, dass es sehr schwierig ist, allgemeine Anforderungen an die Cybersicherheit für alle Eventualitäten festzulegen. Es gilt daher, ein breit gefasstes und allgemeines Konzept der Cybersicherheit für die Zwecke der Zertifizierung zu verabschieden, ergänzt durch besondere Cybersicherheitsziele, die bei der Konzeption der europäischen Systeme für die Cybersicherheitszertifizierung berücksichtigt werden müssen. Die Modalitäten, wie diese Ziele für bestimmte IKT-Produkte und -Dienste erreicht werden, sollten dann weiter im Einzelnen auf der Grundlage des jeweiligen von der Kommission angenommenen Zertifizierungssystems festgelegt werden, etwa durch Verweise auf Normen oder technische Spezifikationen. ***In Abhängigkeit vom jeweiligen Zertifizierungssystem könnte prinzipiell der Rückgriff auf vorhandene bewährte Verfahren bei der Festlegung bestimmter Anforderungen des Systems in Frage kommen.***

Or. en

Begründung

Im Bereich IKT gibt es bereits viele bewährte Verfahren, die in den Sicherheits-Fachkreisen akzeptiert sind und (fast) alle Schwachstellen abdecken. Ein neues System könnte daher auf dem bereits vorhandenen Wissen aufbauen. Wenn es im Interesse der EU liegt, diese bewährten Verfahren zu ändern, dann sollte dies ohne Zweifel leicht zu begründen sein.

Änderungsantrag 101

Nicola Danti, Evelyne Gebhardt, Maria Grapini, Sergio Gutiérrez Prieto, Lucy Anderson, Arndt Kohn, Catherine Stihler, Kerstin Westphal, Pina Picierno, Marc Tarabella, Christel Schaldemose

Vorschlag für eine Verordnung

Erwägung 55 a (neu)

Vorschlag der Kommission

Geänderter Text

(55a) Angesichts der innovativen Entwicklungen und der zunehmenden Verfügbarkeit und ständig wachsenden Zahl an IoT-Geräten in allen Bereichen der Gesellschaft muss ein besonderes Augenmerk auf die Sicherheit aller, auch der einfachsten IoT-Produkte gelegt werden. Da die Zertifizierung ein wichtiges Mittel ist, um das Vertrauen in den Markt sowie die Sicherheit und Abwehrfähigkeit zu steigern, sollte IoT-Produkten und -Diensten im neuen europäischen Rahmen für die Cybersicherheitszertifizierung besondere Aufmerksamkeit zuteilwerden, um sie weniger anfällig und für Verbraucher und Unternehmen sicherer zu machen.

Or. en

Änderungsantrag 102

Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung

Erwägung 56

Vorschlag der Kommission

Geänderter Text

(56) Die Kommission sollte befugt sein, die ENISA mit der Ausarbeitung möglicher Zertifizierungssysteme für bestimmte IKT-Produkte und -Dienste zu beauftragen. Die Kommission sollte dann befugt sein, auf der Grundlage des von der ENISA vorgeschlagenen möglichen Systems das europäische System für die Cybersicherheitszertifizierung mittels eines Durchführungsrechtsakts anzunehmen. Unter Berücksichtigung des allgemeinen Zwecks und der in dieser Verordnung festgelegten Sicherheitsziele sollte in den von der Kommission angenommenen europäischen Systemen für die Cybersicherheitszertifizierung Mindestbestimmungen in Bezug auf den Gegenstand, den Anwendungsbereich und die Funktionsweise des einzelnen Systems festgelegt werden. Hierunter fallen u. a. Anwendungsbereich und Ziel der Cybersicherheitszertifizierung, darunter auch die Kategorien von IKT-Produkten **und** -Diensten, detaillierte Spezifikationen der Anforderungen an die Cybersicherheit, etwa durch Verweise auf Normen oder technische Spezifikationen, die jeweiligen Bewertungskriterien und -verfahren sowie die beabsichtigte Vertrauenswürdigkeitsstufe: „**niedrig**“, „**mittel**“ bzw. „**hoch**“.

(56) Die Kommission sollte befugt sein, die ENISA mit der Ausarbeitung möglicher Zertifizierungssysteme für bestimmte IKT-Produkte und -Dienste zu beauftragen. Die Kommission sollte dann befugt sein, auf der Grundlage des von der ENISA vorgeschlagenen möglichen Systems das europäische System für die Cybersicherheitszertifizierung mittels eines Durchführungsrechtsakts anzunehmen. **Um das Vertrauen in und die Vorhersehbarkeit im Hinblick auf den Rahmen für die Cybersicherheitszertifizierung zu stärken sowie das öffentliche Bewusstsein dessen zu erhöhen, sollte die ENISA eine eigene Website unterhalten, mit einem einfach zu nutzenden Online-Tool, das Informationen zu angenommenen Systemen, möglichen Systemen und von der Kommission angeforderten Systemen auflistet.** Unter Berücksichtigung des allgemeinen Zwecks und der in dieser Verordnung festgelegten Sicherheitsziele sollte in den von der Kommission angenommenen europäischen Systemen für die Cybersicherheitszertifizierung Mindestbestimmungen in Bezug auf den Gegenstand, den Anwendungsbereich und die Funktionsweise des einzelnen Systems festgelegt werden. Hierunter fallen u. a. Anwendungsbereich und Ziel der Cybersicherheitszertifizierung, darunter auch die Kategorien von IKT-Produkten, -Diensten **und -Prozessen**, detaillierte Spezifikationen der Anforderungen an die Cybersicherheit, etwa durch Verweise auf Normen oder technische Spezifikationen, die jeweiligen Bewertungskriterien und -verfahren, **die mit dem Betrieb und der Nutzung von IKT-Produkten, -Prozessen oder -Diensten im Zusammenhang stehen**, sowie die beabsichtigte Vertrauenswürdigkeitsstufe: „**sicher**“, „**ziemlich sicher**“, „**äußerst sicher**“ oder **jegliche Kombinationen daraus**.

Or. en

Änderungsantrag 103

Nicola Danti, Maria Grapini, Sergio Gutiérrez Prieto, Lucy Anderson, Arndt Kohn, Pina Picierno, Marc Tarabella, Christel Schaldemose

Vorschlag für eine Verordnung Erwägung 56

Vorschlag der Kommission

(56) Die Kommission sollte befugt sein, die ENISA mit der Ausarbeitung möglicher Zertifizierungssysteme für bestimmte IKT-Produkte und -Dienste zu beauftragen. **Die Kommission sollte dann befugt sein, auf der Grundlage des von der ENISA vorgeschlagenen möglichen Systems das europäische System für die Cybersicherheitszertifizierung mittels eines Durchführungsrechtsakts anzunehmen. Unter Berücksichtigung des allgemeinen Zwecks und der in dieser Verordnung festgelegten Sicherheitsziele sollte in den von der Kommission angenommenen europäischen Systemen für die Cybersicherheitszertifizierung Mindestbestimmungen in Bezug auf den Gegenstand, den Anwendungsbereich und die Funktionsweise des einzelnen Systems festgelegt werden. Hierunter fallen u. a. Anwendungsbereich und Ziel der Cybersicherheitszertifizierung, darunter auch die Kategorien von IKT-Produkten und -Diensten, detaillierte Spezifikationen der Anforderungen an die Cybersicherheit, etwa durch Verweise auf Normen oder technische Spezifikationen, die jeweiligen Bewertungskriterien und -verfahren sowie die beabsichtigte Vertrauenswürdigkeitsstufe: „niedrig“, „mittel“ bzw. „hoch“.**

Geänderter Text

(56) Die Kommission sollte befugt sein, die ENISA mit der Ausarbeitung möglicher Zertifizierungssysteme für bestimmte IKT-Produkte und -Dienste zu beauftragen. **Der Kommission sollte die Befugnis übertragen werden, gemäß Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union Rechtsakte zur Schaffung europäischer Systeme für die Cybersicherheitszertifizierung für IKT-Produkte und -Dienste zu erlassen. 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. Beim Erlass solcher delegierter Rechtsakte sollte die Kommission den Cybersicherheitszertifizierungssystemen für IKT-Produkte und -Dienste einschlägige Vorschläge der ENISA zu den Systemen zugrunde zu legen.**

Änderungsantrag 104
Anneleen Van Bossuyt, Daniel Dalton

Vorschlag für eine Verordnung
Erwägung 56

Vorschlag der Kommission

(56) Die Kommission sollte befugt sein, die ENISA mit der Ausarbeitung möglicher Zertifizierungssysteme für bestimmte IKT-Produkte und -Dienste zu beauftragen. Die Kommission sollte dann befugt sein, auf der Grundlage des von der ENISA vorgeschlagenen möglichen Systems das europäische System für die Cybersicherheitszertifizierung mittels eines Durchführungsrechtsakts anzunehmen. Unter Berücksichtigung des allgemeinen Zwecks und der in dieser Verordnung festgelegten Sicherheitsziele sollte in den von der Kommission angenommenen europäischen Systemen für die Cybersicherheitszertifizierung Mindestbestimmungen in Bezug auf den Gegenstand, den Anwendungsbereich und die Funktionsweise des einzelnen Systems festgelegt werden. Hierunter fallen u. a. Anwendungsbereich und Ziel der Cybersicherheitszertifizierung, darunter auch die Kategorien von IKT-Produkten und -Diensten, detaillierte Spezifikationen der Anforderungen an die Cybersicherheit, etwa durch Verweise auf Normen oder technische Spezifikationen, die jeweiligen Bewertungskriterien und -verfahren sowie die beabsichtigte Vertrauenswürdigkeitsstufe: „*niedrig*“, „*mittel*“ bzw. „*hoch*“.

Geänderter Text

(56) Die Kommission sollte befugt sein, die ENISA mit der Ausarbeitung möglicher Zertifizierungssysteme für bestimmte IKT-Produkte und -Dienste zu beauftragen. Die Kommission sollte dann befugt sein, auf der Grundlage des von der ENISA vorgeschlagenen möglichen Systems das europäische System für die Cybersicherheitszertifizierung mittels eines Durchführungsrechtsakts anzunehmen. Unter Berücksichtigung des allgemeinen Zwecks und der in dieser Verordnung festgelegten Sicherheitsziele sollte in den von der Kommission angenommenen europäischen Systemen für die Cybersicherheitszertifizierung Mindestbestimmungen in Bezug auf den Gegenstand, den Anwendungsbereich und die Funktionsweise des einzelnen Systems festgelegt werden. Hierunter fallen u. a. Anwendungsbereich und Ziel der Cybersicherheitszertifizierung, darunter auch die Kategorien von IKT-Produkten und -Diensten, detaillierte Spezifikationen der Anforderungen an die Cybersicherheit, etwa durch Verweise auf Normen oder technische Spezifikationen, die jeweiligen Bewertungskriterien und -verfahren sowie die beabsichtigte Vertrauenswürdigkeitsstufe. ***In dem System sollte der komplette Lebenszyklus des Produkts, einschließlich aller für die Außerbetriebnahme von Produkten oder Einstellung von Diensten geltenden Vorschriften, berücksichtigt werden.***

Änderungsantrag 105

Liisa Jaakonsaari, Christel Schaldemose, Lucy Anderson

Vorschlag für eine Verordnung

Erwägung 56

Vorschlag der Kommission

(56) Die Kommission sollte befugt sein, die ENISA mit der Ausarbeitung möglicher Zertifizierungssysteme für bestimmte IKT-Produkte und -Dienste zu beauftragen. Die Kommission sollte dann befugt sein, auf der Grundlage des von der ENISA vorgeschlagenen möglichen Systems das europäische System für die Cybersicherheitszertifizierung mittels eines Durchführungsrechtsakts anzunehmen. Unter Berücksichtigung des allgemeinen Zwecks und der in dieser Verordnung festgelegten Sicherheitsziele sollte in den von der Kommission angenommenen europäischen Systemen für die Cybersicherheitszertifizierung Mindestbestimmungen in Bezug auf den Gegenstand, den Anwendungsbereich und die Funktionsweise des einzelnen Systems festgelegt werden. Hierunter fallen u. a. Anwendungsbereich und Ziel der Cybersicherheitszertifizierung, darunter auch die Kategorien von IKT-Produkten und -Diensten, detaillierte Spezifikationen der Anforderungen an die Cybersicherheit, etwa durch Verweise auf Normen oder technische Spezifikationen, die jeweiligen Bewertungskriterien und -verfahren sowie die beabsichtigte Vertrauenswürdigkeitsstufe: „niedrig“, „mittel“ bzw. „hoch“.

Geänderter Text

(56) Die Kommission sollte befugt sein, die ENISA mit der Ausarbeitung möglicher Zertifizierungssysteme für bestimmte IKT-Produkte und -Dienste zu beauftragen. Die Kommission sollte dann befugt sein, auf der Grundlage des von der ENISA vorgeschlagenen möglichen Systems das europäische System für die Cybersicherheitszertifizierung mittels eines Durchführungsrechtsakts anzunehmen. Unter Berücksichtigung des allgemeinen Zwecks und der in dieser Verordnung festgelegten Sicherheitsziele sollte in den von der Kommission angenommenen europäischen Systemen für die Cybersicherheitszertifizierung Mindestbestimmungen in Bezug auf den Gegenstand, den Anwendungsbereich und die Funktionsweise des einzelnen Systems festgelegt werden. Hierunter fallen u. a. Anwendungsbereich und Ziel der Cybersicherheitszertifizierung, darunter auch die Kategorien von IKT-Produkten und -Diensten, detaillierte Spezifikationen der Anforderungen an die Cybersicherheit, etwa durch Verweise auf Normen oder technische Spezifikationen, die jeweiligen Bewertungskriterien und -verfahren sowie die beabsichtigte Vertrauenswürdigkeitsstufe: „niedrig“, „mittel“ bzw. „hoch“. ***Systeme, die Siegel oder Kennzeichen vorsehen, könnten Unternehmen einen Anreiz bieten, im Bereich Sicherheit bewährte Verfahren anzuwenden.***

Or. en

Änderungsantrag 106
Andreas Schwab, Philippe Juvin

Vorschlag für eine Verordnung
Erwägung 56

Vorschlag der Kommission

(56) Die Kommission sollte befugt sein, die ENISA mit der Ausarbeitung möglicher Zertifizierungssysteme für bestimmte IKT-Produkte und -Dienste zu beauftragen. Die Kommission sollte dann befugt sein, auf der Grundlage des von der ENISA vorgeschlagenen möglichen Systems das europäische System für die Cybersicherheitszertifizierung mittels eines Durchführungsrechtsakts anzunehmen. Unter Berücksichtigung des allgemeinen Zwecks und der in dieser Verordnung festgelegten Sicherheitsziele sollte in den von der Kommission angenommenen europäischen Systemen für die Cybersicherheitszertifizierung Mindestbestimmungen in Bezug auf den Gegenstand, den Anwendungsbereich und die Funktionsweise des einzelnen Systems festgelegt werden. Hierunter fallen u. a. Anwendungsbereich und Ziel der Cybersicherheitszertifizierung, darunter auch die Kategorien von IKT-Produkten und -Diensten, detaillierte Spezifikationen der Anforderungen an die Cybersicherheit, etwa durch Verweise auf Normen oder technische Spezifikationen, die jeweiligen Bewertungskriterien und -verfahren sowie die beabsichtigte Vertrauenswürdigkeitsstufe: „niedrig“, „mittel“ bzw. „hoch“.

Geänderter Text

(56) Die Kommission sollte befugt sein, die ENISA mit der Ausarbeitung möglicher Zertifizierungssysteme für bestimmte IKT-Produkte und -Dienste zu beauftragen. Die Kommission sollte dann befugt sein, auf der Grundlage des von der ENISA vorgeschlagenen möglichen Systems das europäische System für die Cybersicherheitszertifizierung mittels eines Durchführungsrechtsakts anzunehmen. Unter Berücksichtigung des allgemeinen Zwecks und der in dieser Verordnung festgelegten Sicherheitsziele sollte in den von der Kommission angenommenen europäischen Systemen für die Cybersicherheitszertifizierung Mindestbestimmungen in Bezug auf den Gegenstand, den Anwendungsbereich und die Funktionsweise des einzelnen Systems festgelegt werden. Hierunter fallen u. a. Anwendungsbereich und Ziel der Cybersicherheitszertifizierung, darunter auch die Kategorien von IKT-Produkten und -Diensten, detaillierte Spezifikationen der Anforderungen an die Cybersicherheit, etwa durch Verweise auf Normen oder technische Spezifikationen, die jeweiligen Bewertungskriterien und -verfahren sowie die beabsichtigte Vertrauenswürdigkeitsstufe: „niedrig“, „mittel“ bzw. „hoch“. **Die Sicherheitsanforderungen sollten mit den Risiken im Zusammenhang stehen, die sich aus dem IKT-Produkt oder -Dienst ergeben.**

Or. en

Änderungsantrag 107

Mylène Troszczynski

Vorschlag für eine Verordnung
Erwägung 56

Vorschlag der Kommission

(56) Die Kommission sollte befugt sein, die ENISA mit der Ausarbeitung möglicher Zertifizierungssysteme für bestimmte IKT-Produkte und -Dienste zu beauftragen. Die Kommission **sollte** dann befugt **sein**, auf der Grundlage des von der ENISA vorgeschlagenen möglichen Systems das europäische System für die Cybersicherheitszertifizierung mittels eines Durchführungsrechtsakts anzunehmen. Unter Berücksichtigung des allgemeinen Zwecks und der in dieser Verordnung festgelegten Sicherheitsziele **sollte** in den von der Kommission angenommenen europäischen Systemen für die Cybersicherheitszertifizierung Mindestbestimmungen in Bezug auf den Gegenstand, den Anwendungsbereich und die Funktionsweise des einzelnen Systems festgelegt werden. Hierunter fallen u. a. Anwendungsbereich und Ziel der Cybersicherheitszertifizierung, darunter auch die Kategorien von IKT-Produkten und -Diensten, detaillierte Spezifikationen der Anforderungen an die Cybersicherheit, etwa durch Verweise auf Normen oder technische Spezifikationen, die jeweiligen Bewertungskriterien und -verfahren sowie die beabsichtigte Vertrauenswürdigkeitsstufe: „niedrig“, „mittel“ bzw. „hoch“.

Geänderter Text

(56) Die Kommission sollte befugt sein, die ENISA mit der Ausarbeitung möglicher Zertifizierungssysteme für bestimmte IKT-Produkte und -Dienste zu beauftragen. Die Kommission **wäre** dann befugt, auf der Grundlage des von der ENISA vorgeschlagenen möglichen Systems das europäische System für die Cybersicherheitszertifizierung **erst nach Erhalt der Zustimmung der Mitgliedstaaten** mittels eines Durchführungsrechtsakts anzunehmen. Unter Berücksichtigung des allgemeinen Zwecks und der in dieser Verordnung festgelegten Sicherheitsziele **sollten** in den von der Kommission angenommenen europäischen Systemen für die Cybersicherheitszertifizierung Mindestbestimmungen in Bezug auf den Gegenstand, den Anwendungsbereich und die Funktionsweise des einzelnen Systems festgelegt werden. Hierunter fallen u. a. Anwendungsbereich und Ziel der Cybersicherheitszertifizierung, darunter auch die Kategorien von IKT-Produkten und -Diensten, detaillierte Spezifikationen der Anforderungen an die Cybersicherheit, etwa durch Verweise auf Normen oder technische Spezifikationen, die jeweiligen Bewertungskriterien und -verfahren sowie die beabsichtigte Vertrauenswürdigkeitsstufe: „niedrig“, „mittel“ bzw. „hoch“.

Or. fr

Änderungsantrag 108
Roberta Metsola

Vorschlag für eine Verordnung

Erwägung 56

Vorschlag der Kommission

(56) Die Kommission sollte befugt sein, die ENISA mit der Ausarbeitung möglicher Zertifizierungssysteme für bestimmte IKT-Produkte und -Dienste zu beauftragen. Die Kommission sollte dann befugt sein, auf der Grundlage des von der ENISA vorgeschlagenen möglichen Systems das europäische System für die Cybersicherheitszertifizierung mittels eines Durchführungsrechtsakts anzunehmen. Unter Berücksichtigung des allgemeinen Zwecks und der in dieser Verordnung festgelegten Sicherheitsziele sollte in den von der Kommission angenommenen europäischen Systemen für die Cybersicherheitszertifizierung Mindestbestimmungen in Bezug auf den Gegenstand, den Anwendungsbereich und die Funktionsweise des einzelnen Systems festgelegt werden. Hierunter fallen u. a. Anwendungsbereich und Ziel der Cybersicherheitszertifizierung, darunter auch die Kategorien von **IKT-Produkten und -Diensten**, detaillierte Spezifikationen der Anforderungen an die Cybersicherheit, etwa durch Verweise auf Normen oder technische Spezifikationen, die jeweiligen Bewertungskriterien und -verfahren sowie die beabsichtigte Vertrauenswürdigkeitsstufe: „**niedrig**“, „mittel“ bzw. „hoch“.

Geänderter Text

(56) Die Kommission sollte befugt sein, die ENISA mit der Ausarbeitung möglicher Zertifizierungssysteme für bestimmte IKT-Produkte und -Dienste zu beauftragen. Die Kommission sollte dann befugt sein, auf der Grundlage des von der ENISA vorgeschlagenen möglichen Systems das europäische System für die Cybersicherheitszertifizierung mittels eines Durchführungsrechtsakts anzunehmen. Unter Berücksichtigung des allgemeinen Zwecks und der in dieser Verordnung festgelegten Sicherheitsziele sollte in den von der Kommission angenommenen europäischen Systemen für die Cybersicherheitszertifizierung Mindestbestimmungen in Bezug auf den Gegenstand, den Anwendungsbereich und die Funktionsweise des einzelnen Systems festgelegt werden. Hierunter fallen u. a. Anwendungsbereich und Ziel der Cybersicherheitszertifizierung, darunter auch die Kategorien von **IKT-Hardware- und Software-Produkten und -Diensten**, detaillierte Spezifikationen der Anforderungen an die Cybersicherheit, etwa durch Verweise auf Normen oder technische Spezifikationen, die jeweiligen Bewertungskriterien und -verfahren sowie die beabsichtigte **risikobasierte** Vertrauenswürdigkeitsstufe: „**grundlegend**“, „mittel“ bzw. „hoch“.

Or. en

Änderungsantrag 109

Nicola Danti, Evelyne Gebhardt, Maria Grapini, Sergio Gutiérrez Prieto, Lucy Anderson, Arndt Kohn, Catherine Stihler, Kerstin Westphal, Pina Picierno, Marc Tarabella

**Vorschlag für eine Verordnung
Erwägung 56 a (neu)**

Vorschlag der Kommission

Geänderter Text

(56a) Unter den Bewertungsmethoden und -verfahren für jedes europäische System für die Cybersicherheitszertifizierung sollte ethisches Hacking – bei dem Schwachstellen und Anfälligkeiten von Geräten und Informationssystemen durch das Antizipieren der möglichen Handlungen und Fertigkeiten von Hackern mit böswilligen Absichten aufgespürt werden sollen – auf Unionsebene gefördert werden.

Or. en

Änderungsantrag 110
Maria Grapini

Vorschlag für eine Verordnung
Erwägung 56 a (neu)

Vorschlag der Kommission

Geänderter Text

(56a) Eine Überprüfung des europäischen Zertifizierungsverfahren ist notwendig, um einen Anstieg der Kosten für die Hersteller zu vermeiden.

Or. ro

Änderungsantrag 111
Jiří Pospíšil

Vorschlag für eine Verordnung
Erwägung 57

Vorschlag der Kommission

Geänderter Text

(57) Der Rückgriff auf eine europäische Cybersicherheitszertifizierung sollte freiwillig bleiben, sofern im Unionsrecht oder im einzelstaatlichen Recht nichts anderes festgelegt ist. Mit Blick auf die

(57) Der Rückgriff auf eine europäische Cybersicherheitszertifizierung sollte freiwillig bleiben, sofern im Unionsrecht oder im einzelstaatlichen Recht nichts anderes festgelegt ist. Mit Blick auf die

Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, jedoch ab dem Zeitpunkt unwirksam werden, den die Kommission in einem Durchführungsrechtsakt festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung der IKT-Produkte und -Dienste einführen, die bereits unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen.

Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, jedoch ab dem Zeitpunkt unwirksam werden, den die Kommission in einem Durchführungsrechtsakt festlegt, **und zwar mit Ausnahme von Fällen der nationalen Sicherheit der Staaten, der Verarbeitung von Verschlusssachen und der nationalen Sicherheit und damit verbundener öffentlicher Aufträge. Dies sollte ab dem von der Kommission in einem Durchführungsrechtsakt festgelegten Datum erfolgen, wobei den Mitgliedstaaten ausreichend Zeit für einen ruhigen und problemlosen Übergang zum neuen Zertifizierungssystem eingeräumt werden sollte.** Zudem sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung der IKT-Produkte und -Dienste einführen, die bereits unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen. **Das vorgeschlagene Zertifizierungssystem sollte daher in einem Umfeld sich schnell entwickelnder Technologien ausreichend flexibel und wirksam anpassbar sein, die Vereinbarkeit mit internationalen Standards sollte gewährleistet sein und es sollten keine Innovationshemmnisse geschaffen werden, damit das System für die Mitgliedstaaten einen tatsächlichen Nutzen darstellt und keinesfalls Schwierigkeiten mit sich bringt.**

Or. cs

Änderungsantrag 112
Jiří Maštálka

Vorschlag für eine Verordnung

Erwägung 57

Vorschlag der Kommission

(57) Der Rückgriff auf eine europäische Cybersicherheitszertifizierung sollte freiwillig bleiben, sofern im Unionsrecht oder im einzelstaatlichen Recht nichts anderes festgelegt ist. Mit Blick auf die Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, jedoch ab dem Zeitpunkt unwirksam werden, den die Kommission in einem Durchführungsrechtsakt festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung der IKT-Produkte und -Dienste einführen, die bereits unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen.

Geänderter Text

(57) Der Rückgriff auf eine europäische Cybersicherheitszertifizierung sollte freiwillig bleiben, sofern im Unionsrecht oder im einzelstaatlichen Recht nichts anderes festgelegt ist. ***Es ist davon auszugehen, dass – nach dieser Anfangsphase und in Abhängigkeit von der Umsetzung in den Mitgliedstaaten der EU sowie dem Stellenwert eines Produkts oder Dienstes – für künftige Technologiegenerationen stufenweise verbindliche Systeme für IKT-Produkte und -Dienste entwickelt werden.*** Mit Blick auf die Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, jedoch ab dem Zeitpunkt unwirksam werden, den die Kommission in einem Durchführungsrechtsakt festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung der IKT-Produkte und -Dienste einführen, die bereits unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen. ***Dies gilt jedoch unbeschadet nationaler Systeme, die IKT-Produkte, -Prozesse und -Dienste abdecken und die von den Mitgliedstaaten für ihre eigenen souveränen Zwecke genutzt werden. Für diese Systeme tragen allein die Mitgliedstaaten die Verantwortung.***

Or. en

Änderungsantrag 113

Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung
Erwägung 57

Vorschlag der Kommission

(57) Der Rückgriff auf eine europäische Cybersicherheitszertifizierung sollte freiwillig bleiben, sofern im Unionsrecht oder im einzelstaatlichen Recht nichts anderes festgelegt ist. Mit Blick auf die Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, **jedoch** ab dem Zeitpunkt unwirksam werden, den die Kommission in einem Durchführungsrechtsakt festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung der IKT-Produkte und -Dienste einführen, die bereits unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen.

Geänderter Text

(57) Der Rückgriff auf eine europäische Cybersicherheitszertifizierung sollte freiwillig bleiben, sofern im Unionsrecht oder im einzelstaatlichen Recht nichts anderes festgelegt ist.
Grundanforderungen im Bereich der IT-Sicherheit müssen jedoch verbindlich sein und für alle Geräte und Dienste für Verbraucher umgesetzt werden, um die Herausforderungen unserer immer stärker vernetzten Welt zu meistern. Diese Mindestanforderungen könnten die Authentifizierung, die Sicherheit von Verbindungen und Fehlerkorrekturen für entdeckte Schwachstellen umfassen. Mit Blick auf die Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, ab dem Zeitpunkt unwirksam werden, den die Kommission in einem Durchführungsrechtsakt festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung der IKT-Produkte und -Dienste einführen, die bereits unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen.

Or. en

Begründung

Mit dieser Ergänzung soll der derzeitige Mangel an einheitlichen Grundanforderungen im Bereich IT-Sicherheit schnell behoben werden.

Änderungsantrag 114
Anneleen Van Bossuyt, Daniel Dalton

Vorschlag für eine Verordnung
Erwägung 57

Vorschlag der Kommission

(57) Der Rückgriff auf eine europäische Cybersicherheitszertifizierung sollte freiwillig bleiben, **sofern** im Unionsrecht **oder im einzelstaatlichen Recht nichts anderes** festgelegt ist. Mit Blick auf die Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, **jedoch** ab dem Zeitpunkt unwirksam werden, den die Kommission in einem Durchführungsrechtsakt festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung der IKT-Produkte und -Dienste einführen, die bereits unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen.

Geänderter Text

(57) Der Rückgriff auf eine europäische Cybersicherheitszertifizierung sollte freiwillig bleiben. **Wenn im EU-Recht die Erfordernis entsteht, für bestimmte Produkte oder Dienste die Einhaltung einer Reihe von einheitlichen Cybersicherheitsanforderungen nachzuweisen, sollten die Anforderungen sowie das Verfahren zur Bewertung und Überprüfung der Einhaltung im Einklang mit dem Neuen Ansatz** im Unionsrecht festgelegt **werden**. Mit Blick auf die Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, ab dem Zeitpunkt unwirksam werden, den die Kommission in einem Durchführungsrechtsakt festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung der IKT-Produkte und -Dienste einführen, die bereits unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen.

Or. en

Änderungsantrag 115
Dita Charanzová

Vorschlag für eine Verordnung
Erwägung 57

Vorschlag der Kommission

(57) Der Rückgriff auf eine europäische Cybersicherheitszertifizierung sollte freiwillig bleiben, **sofern im Unionsrecht oder im einzelstaatlichen Recht nichts anderes festgelegt ist**. Mit Blick auf die Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, **jedoch** ab dem Zeitpunkt unwirksam werden, den die Kommission in einem Durchführungsrechtsakt festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung der IKT-Produkte und -Dienste einführen, die bereits unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen.

Geänderter Text

(57) Der Rückgriff auf eine europäische Cybersicherheitszertifizierung sollte freiwillig bleiben. **Dies sollte die Union und die Verwaltungen der Mitgliedstaaten jedoch nicht davon abhalten, eine europäische Cybersicherheitszertifizierung unter anderem im Rahmen der Genehmigung von Infrastrukturprojekten oder öffentlichen Aufträgen zu verlangen**. Mit Blick auf die Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, ab dem Zeitpunkt unwirksam werden, den die Kommission in einem Durchführungsrechtsakt festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung der IKT-Produkte und -Dienste einführen, die bereits unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen.

Or. en

Änderungsantrag 116
Andreas Schwab, Philippe Juvin

Vorschlag für eine Verordnung
Erwägung 57

Vorschlag der Kommission

(57) Der Rückgriff auf eine europäische Cybersicherheitszertifizierung sollte freiwillig bleiben, sofern im Unionsrecht oder im einzelstaatlichen Recht nichts anderes festgelegt ist. Mit Blick auf die

Geänderter Text

(57) Der Rückgriff auf eine europäische Cybersicherheitszertifizierung sollte freiwillig bleiben, **mit Ausnahme von IKT-Produkten und -Diensten mit hohen Sicherheitsanforderungen und** sofern im

Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, jedoch ab dem Zeitpunkt unwirksam werden, den die Kommission in einem Durchführungsrechtsakt festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung der IKT-Produkte und -Dienste einführen, die bereits unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen.

Unionsrecht oder im einzelstaatlichen Recht nichts anderes festgelegt ist. Mit Blick auf die Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, jedoch ab dem Zeitpunkt unwirksam werden, den die Kommission in einem Durchführungsrechtsakt festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung der IKT-Produkte und -Dienste einführen, die bereits unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen.

Or. en

Änderungsantrag 117 **Dennis de Jong**

Vorschlag für eine Verordnung **Erwägung 57**

Vorschlag der Kommission

(57) **Der Rückgriff auf eine europäische** Cybersicherheitszertifizierung sollte **freiwillig bleiben**, sofern im Unionsrecht **oder im einzelstaatlichen Recht** nichts anderes festgelegt ist. Mit Blick auf die Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, jedoch ab dem Zeitpunkt unwirksam werden, den die Kommission in einem Durchführungsrechtsakt festlegt. Zudem

Geänderter Text

(57) **Die Grundanforderungen im Bereich IT-Sicherheit sollten in einem europäischen Rahmen für die** Cybersicherheitszertifizierung **geregelt werden, der verbindlich sein** sollte, sofern im Unionsrecht nichts anderes festgelegt ist. Mit Blick auf die Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, jedoch ab dem Zeitpunkt unwirksam werden, den die Kommission in einem

sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung der IKT-Produkte und -Dienste einführen, die bereits unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen.

Durchführungsrechtsakt festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung der IKT-Produkte und -Dienste einführen, die bereits unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen.

Or. en

Änderungsantrag 118 **Lambert van Nistelrooij**

Vorschlag für eine Verordnung **Erwägung 57**

Vorschlag der Kommission

(57) **Der Rückgriff auf eine europäische** Cybersicherheitszertifizierung sollte **freiwillig bleiben**, sofern im Unionsrecht **oder im einzelstaatlichen Recht** nichts anderes festgelegt ist. Mit Blick auf die Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, jedoch ab dem Zeitpunkt unwirksam werden, den die Kommission in einem Durchführungsrechtsakt festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung der IKT-Produkte und -Dienste einführen, die bereits unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen.

Geänderter Text

(57) **Die Grundanforderungen im Bereich IT-Sicherheit sollten in einem europäischen Rahmen für die** Cybersicherheitszertifizierung **geregelt werden, der verbindlich sein** sollte, sofern im Unionsrecht nichts anderes festgelegt ist. Mit Blick auf die Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, jedoch ab dem Zeitpunkt unwirksam werden, den die Kommission in einem Durchführungsrechtsakt festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung der IKT-Produkte und -Dienste einführen, die bereits unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen.

Or. en

Begründung

Voluntary certification will not tackle the introduction of new unsafe ICT products and services. For instance, the number of connected (consumer and business) IoT-devices will grow with millions in the oncoming years. Competition for these products is price based, less on certifications. When ICT products and services don't comply to baseline ICT security requirements they will be used for botnets, remain vulnerable for hacks and privacy infringements. A voluntary certification framework therefore will not solve this issue. It will only work when implemented probably as an mandatory and EU harmonized framework.

Änderungsantrag 119 **Roberta Metsola**

Vorschlag für eine Verordnung **Erwägung 57**

Vorschlag der Kommission

(57) Der Rückgriff auf eine europäische Cybersicherheitszertifizierung sollte freiwillig bleiben, sofern im Unionsrecht oder im einzelstaatlichen Recht nichts anderes festgelegt ist. Mit Blick auf die Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, jedoch ab dem Zeitpunkt unwirksam werden, den die Kommission in einem Durchführungsrechtsakt festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung der **IKT-Produkte und -Dienste** einführen, die bereits unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen.

Geänderter Text

(57) Der Rückgriff auf eine europäische Cybersicherheitszertifizierung sollte freiwillig bleiben, sofern im Unionsrecht oder im einzelstaatlichen Recht nichts anderes festgelegt ist. Mit Blick auf die Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte und -Dienste, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, jedoch ab dem Zeitpunkt unwirksam werden, den die Kommission in einem Durchführungsrechtsakt festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Systeme für die Cybersicherheitszertifizierung der **IKT-Hardware- und Software-Produkte und -Dienste** einführen, die bereits unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen.

Or. en

Änderungsantrag 120
Roberta Metsola

Vorschlag für eine Verordnung
Erwägung 58

Vorschlag der Kommission

(58) Sobald ein europäisches System für die Cybersicherheitszertifizierung verabschiedet worden ist, sollten Hersteller von **IKT-Produkten** und Anbieter von IKT-Diensten die Zertifizierung ihrer Produkte oder Dienste bei einer Konformitätsbewertungsstelle ihrer Wahl beantragen können. Die Konformitätsbewertungsstellen sollten, sofern sie bestimmten in dieser Verordnung festgelegten Anforderungen genügen, von einer Akkreditierungsstelle akkreditiert werden. Die Akkreditierung sollte für eine **Höchstdauer von fünf Jahren** erfolgen und unter denselben Bedingungen verlängert werden können, sofern die Konformitätsbewertungsstelle die Anforderungen erfüllt. Die Akkreditierungsstellen sollten die einer Konformitätsbewertungsstelle erteilte Akkreditierung widerrufen, wenn die Voraussetzungen für die Akkreditierung nicht oder nicht mehr erfüllt werden oder wenn eine Konformitätsbewertungsstelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind.

Geänderter Text

(58) Sobald ein europäisches System für die Cybersicherheitszertifizierung verabschiedet worden ist, sollten Hersteller von **IKT-Hardware- oder Software-Produkten** und Anbieter von IKT-Diensten die Zertifizierung ihrer Produkte oder Dienste bei einer Konformitätsbewertungsstelle ihrer Wahl beantragen können. **Die Hersteller können sich auch für eine Konformitäts-Eigenerklärung über die Einhaltung des entsprechenden europäischen Systems für die Cybersicherheitszertifizierung entscheiden und unterliegen dann der Kontrolle der nationalen Aufsichtsbehörde für die Zertifizierung, die wiederum die Ergebnisse ihrer Beurteilungen der Europäischen Gruppe für die Cybersicherheitszertifizierung und der ENISA meldet.** Die Konformitätsbewertungsstellen sollten, sofern sie bestimmten in dieser Verordnung festgelegten Anforderungen genügen, von einer Akkreditierungsstelle akkreditiert werden. Die Akkreditierung sollte für eine **im entsprechenden europäischen System für die Cybersicherheitszertifizierung festgelegte Dauer** erfolgen und unter denselben Bedingungen verlängert werden können, sofern die Konformitätsbewertungsstelle die Anforderungen erfüllt. Die Akkreditierungsstellen sollten die einer Konformitätsbewertungsstelle erteilte Akkreditierung widerrufen, wenn die Voraussetzungen für die Akkreditierung nicht oder nicht mehr erfüllt werden oder wenn eine Konformitätsbewertungsstelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind.

Änderungsantrag 121
Andreas Schwab, Philippe Juvin

Vorschlag für eine Verordnung
Erwägung 58

Vorschlag der Kommission

(58) Sobald ein europäisches System für die Cybersicherheitszertifizierung verabschiedet worden ist, sollten Hersteller von IKT-Produkten und Anbieter von IKT-Diensten die Zertifizierung ihrer Produkte oder Dienste bei einer Konformitätsbewertungsstelle ihrer Wahl beantragen können. Die Konformitätsbewertungsstellen sollten, sofern sie bestimmten in dieser Verordnung festgelegten Anforderungen genügen, von einer Akkreditierungsstelle akkreditiert werden. Die Akkreditierung sollte für eine Höchstdauer von fünf Jahren erfolgen und unter denselben Bedingungen verlängert werden können, sofern die Konformitätsbewertungsstelle die Anforderungen erfüllt. Die Akkreditierungsstellen sollten die einer Konformitätsbewertungsstelle erteilte Akkreditierung widerrufen, wenn die Voraussetzungen für die Akkreditierung nicht oder nicht mehr erfüllt werden oder wenn eine Konformitätsbewertungsstelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind.

Geänderter Text

(58) Sobald ein europäisches System für die Cybersicherheitszertifizierung verabschiedet worden ist, sollten Hersteller von IKT-Produkten und Anbieter von IKT-Diensten die Zertifizierung ihrer Produkte oder Dienste bei einer Konformitätsbewertungsstelle ihrer Wahl beantragen können. **Produkte und Dienste mit hohen Sicherheitsanforderungen müssen zwingend von einem Dritten zertifiziert werden. Für alle anderen IKT-Produkte und -Dienste ist die Zertifizierung durch einen Dritten freiwillig, sofern nicht anderweitig im Unionsrecht festgelegt.** Die Konformitätsbewertungsstellen sollten, sofern sie bestimmten in dieser Verordnung festgelegten Anforderungen genügen, von einer Akkreditierungsstelle akkreditiert werden. Die Akkreditierung sollte für eine Höchstdauer von fünf Jahren erfolgen und unter denselben Bedingungen verlängert werden können, sofern die Konformitätsbewertungsstelle die Anforderungen erfüllt. Die Akkreditierungsstellen sollten die einer Konformitätsbewertungsstelle erteilte Akkreditierung widerrufen, wenn die Voraussetzungen für die Akkreditierung nicht oder nicht mehr erfüllt werden oder wenn eine Konformitätsbewertungsstelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind.

Änderungsantrag 122
Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Erwägung 58

Vorschlag der Kommission

(58) Sobald ein europäisches System für die Cybersicherheitszertifizierung verabschiedet worden ist, sollten Hersteller von IKT-Produkten und Anbieter von IKT-Diensten die Zertifizierung ihrer Produkte **oder** Dienste bei einer Konformitätsbewertungsstelle ihrer Wahl beantragen können. Die Konformitätsbewertungsstellen sollten, sofern sie bestimmten in dieser Verordnung festgelegten Anforderungen genügen, von einer Akkreditierungsstelle akkreditiert werden. Die Akkreditierung sollte für eine Höchstdauer von fünf Jahren erfolgen und unter denselben Bedingungen verlängert werden können, sofern die Konformitätsbewertungsstelle die Anforderungen erfüllt. Die Akkreditierungsstellen sollten die einer Konformitätsbewertungsstelle erteilte Akkreditierung widerrufen, wenn die Voraussetzungen für die Akkreditierung nicht oder nicht mehr erfüllt werden oder wenn eine Konformitätsbewertungsstelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind.

Geänderter Text

(58) Sobald ein europäisches System für die Cybersicherheitszertifizierung verabschiedet worden ist, sollten Hersteller von IKT-Produkten und Anbieter von IKT-Diensten die Zertifizierung ihrer Produkte, Dienste **oder Prozesse** bei einer Konformitätsbewertungsstelle ihrer Wahl beantragen können. Die Konformitätsbewertungsstellen sollten, sofern sie bestimmten in dieser Verordnung festgelegten Anforderungen genügen, von einer Akkreditierungsstelle akkreditiert werden. Die Akkreditierung sollte für eine Höchstdauer von fünf Jahren erfolgen und unter denselben Bedingungen verlängert werden können, sofern die Konformitätsbewertungsstelle die Anforderungen erfüllt. Die Akkreditierungsstellen sollten die einer Konformitätsbewertungsstelle erteilte Akkreditierung widerrufen, wenn die Voraussetzungen für die Akkreditierung nicht oder nicht mehr erfüllt werden oder wenn eine Konformitätsbewertungsstelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind.

Or. en

Änderungsantrag 123
Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung
Erwägung 58 a (neu)

Vorschlag der Kommission

Geänderter Text

(58a) Die Agentur sollte klare

obligatorische Grundanforderungen im Bereich der IT-Sicherheit ermitteln, die für alle in der Union verkauften oder aus der Union ausgeführten IT-Geräte gelten, und diese der Kommission gegebenenfalls als Durchführungsrechtsakte vorschlagen. Diese Anforderungen sollten binnen zwei Jahren nach Inkrafttreten dieser Verordnung entwickelt und im Anschluss daran alle zwei Jahre überarbeitet werden, um für eine kontinuierliche und dynamische Verbesserung zu sorgen. Die Grundanforderungen im Bereich der IT-Sicherheit sollten u. a. vorschreiben, dass ein Gerät keine bekannten Sicherheitslücken enthält, dass bei ihm Sicherheitsaktualisierungen aus vertrauenswürdigen Quellen vorgenommen werden können, dass der Anbieter den zuständigen Behörden bekannte Schwachstellen meldet und betroffene Geräte repariert bzw. austauscht und dass der Anbieter darüber informiert, wenn die Sicherheitsunterstützung für ein Gerät ausläuft.

Or. en

Begründung

Es muss eine robuste IT-Umgebung geschaffen werden, um sich vor Computerkriminalität zu schützen und um die Grundrechte der IT-Nutzer zu wahren. Daher sollten mit dieser Verordnung auf hoher Ebene IT-Sicherheitsziele festgelegt werden, die auf obligatorische Vorkehrungen im Bereich der IT-Sicherheit ausgerichtet sind.

Änderungsantrag 124
Roberta Metsola

Vorschlag für eine Verordnung
Erwägung 58 a (neu)

Vorschlag der Kommission

Geänderter Text

(58a) Um sicherzustellen, dass die Akkreditierung in der ganzen

Europäischen Union einheitlich erfolgt, sollten sich die nationalen Akkreditierungsstellen einer durch die ENISA koordinierten gegenseitigen Begutachtung unterziehen.

Or. en

Änderungsantrag 125
Roberta Metsola

Vorschlag für eine Verordnung
Erwägung 59

Vorschlag der Kommission

(59) Es ist notwendig, alle Mitgliedstaaten zur Benennung einer Aufsichtsbehörde für die Cybersicherheitszertifizierung zu verpflichten, die die in ihrem Hoheitsgebiet ansässigen Konformitätsbewertungsstellen und die von diesen ausgestellten Zertifikate im Hinblick auf die Einhaltung der Anforderungen beaufsichtigt, die in dieser Verordnung und in den jeweiligen Cybersicherheitszertifizierungssystemen festgelegt sind. Die nationalen Aufsichtsbehörden für die Zertifizierung sollten Beschwerden, die von natürlichen oder juristischen Personen in Bezug auf die von Konformitätsbewertungsstellen in ihrem Hoheitsgebiet ausgestellten Zertifikate eingereicht werden, bearbeiten, den Beschwerdegegenstand, soweit angemessen, untersuchen und den Beschwerdeführer über die Fortschritte und das Ergebnis der Untersuchung innerhalb einer angemessenen Frist unterrichten. Darüber hinaus sollten sie mit anderen nationalen Aufsichtsbehörden für die Zertifizierung und anderen öffentlichen Stellen zusammenarbeiten, auch indem sie Informationen über die etwaige Nichtkonformität von **IKT-Produkten und -Diensten** mit den Anforderungen dieser Verordnung oder bestimmten europäischen

Geänderter Text

(59) Es ist notwendig, alle Mitgliedstaaten zur Benennung einer Aufsichtsbehörde für die Cybersicherheitszertifizierung zu verpflichten, die die in ihrem Hoheitsgebiet ansässigen Konformitätsbewertungsstellen und die von diesen ausgestellten Zertifikate im Hinblick auf die Einhaltung der Anforderungen beaufsichtigt, die in dieser Verordnung und in den jeweiligen Cybersicherheitszertifizierungssystemen festgelegt sind. Die nationalen Aufsichtsbehörden für die Zertifizierung sollten Beschwerden, die von natürlichen oder juristischen Personen in Bezug auf die von Konformitätsbewertungsstellen in ihrem Hoheitsgebiet ausgestellten Zertifikate eingereicht werden, bearbeiten, den Beschwerdegegenstand, soweit angemessen, untersuchen und den Beschwerdeführer über die Fortschritte und das Ergebnis der Untersuchung innerhalb einer angemessenen Frist unterrichten. Darüber hinaus sollten sie mit anderen nationalen Aufsichtsbehörden für die Zertifizierung und anderen öffentlichen Stellen zusammenarbeiten, auch indem sie Informationen über die etwaige Nichtkonformität von **IKT-Hardware- und Software Produkten und -Diensten** mit den Anforderungen dieser Verordnung

Systemen für die
Cybersicherheitszertifizierung austauschen.

oder bestimmten europäischen Systemen
für die Cybersicherheitszertifizierung
austauschen. ***Des Weiteren sollten sie
kontrollieren und überprüfen, ob die
Konformitäts-Eigenerklärungen
ordnungsmäßig sind und ob europäische
Cybersicherheitszertifikate von
Konformitätsbewertungsstellen anhand
der in dieser Verordnung festgelegten
Anforderungen ausgestellt werden,
darunter die von der Europäischen
Gruppe für die
Cybersicherheitszertifizierung
aufgestellten Regeln und die im
entsprechenden europäischen System für
die Cybersicherheitszertifizierung
festgelegten Anforderungen.***

Or. en

Änderungsantrag 126
Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Erwägung 65

Vorschlag der Kommission

(65) Die Durchführungsrechtsakte über die europäischen Systeme für die Cybersicherheitszertifizierung von IKT-Produkten **und** -Diensten, die Modalitäten für die Durchführung von Umfragen durch die Agentur sowie die Umstände, Formate und Verfahren der Notifizierung akkreditierter Konformitätsbewertungsstellen durch die nationalen Aufsichtsbehörden für die Zertifizierung bei der Kommission sollten nach dem Prüfverfahren erlassen werden.

Geänderter Text

(65) Die Durchführungsrechtsakte über die europäischen Systeme für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten **und -Prozessen**, die Modalitäten für die Durchführung von Umfragen durch die Agentur sowie die Umstände, Formate und Verfahren der Notifizierung akkreditierter Konformitätsbewertungsstellen durch die nationalen Aufsichtsbehörden für die Zertifizierung bei der Kommission sollten nach dem Prüfverfahren erlassen werden.

Or. en

Änderungsantrag 127
Jiří Pospíšil

Vorschlag für eine Verordnung
Erwägung 66

Vorschlag der Kommission

(66) Die Tätigkeit der Agentur sollte unabhängig bewertet werden. Die Bewertung sollte **sich darauf beziehen, inwieweit die** Agentur **ihre Ziele erreicht**, wie sie arbeitet und inwieweit ihre Aufgaben relevant sind. Zudem sollten Wirkung, Wirksamkeit und Effizienz des europäischen Rahmens für Cybersicherheitszertifizierung bewertet werden.

Geänderter Text

(66) Die Tätigkeit der Agentur sollte unabhängig bewertet werden. Die Bewertung sollte **die Richtigkeit und Zweckmäßigkeit der von der** Agentur **eingesetzten Mittel, die Wirksamkeit beim Erreichen ihrer Ziele und eine Beschreibung dessen**, wie sie arbeitet und inwieweit ihre Aufgaben relevant sind, **umfassen**. Zudem sollten Wirkung, Wirksamkeit und Effizienz des europäischen Rahmens für Cybersicherheitszertifizierung bewertet werden.

Or. cs

Änderungsantrag 128
Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung
Artikel 1 – Absatz 1 – Buchstabe a

Vorschlag der Kommission

(a) die Ziele, Aufgaben und organisatorischen Aspekte der „**EU-Cybersicherheitsagentur**“ (ENISA), **im Folgenden** die „Agentur“ und

Geänderter Text

(a) die Ziele, Aufgaben und organisatorischen Aspekte der „**Agentur der Europäischen Union für Netz- und Informationssicherheit**“ (ENISA) (die „Agentur“) und

Or. en

Begründung

Es wird vorgeschlagen, die ursprüngliche Bezeichnung der ENISA (Agentur der Europäischen Union für Netz- und Informationssicherheit) beizubehalten.

Änderungsantrag 129

Vorschlag für eine Verordnung
Artikel 1 – Absatz 1 – Buchstabe b

Vorschlag der Kommission

(b) ein Rahmen für die Festlegung europäischer Zertifizierungssysteme für die Cybersicherheit, mit dem für IKT-Produkte und Dienste in der Union ein angemessenes Maß an Cybersicherheit gewährleistet werden soll. Dieser Rahmen gilt unbeschadet der in anderen Rechtsakten der Union festgelegten Bestimmungen in Bezug auf eine freiwillige oder verbindliche Zertifizierung.

Geänderter Text

(b) ein Rahmen für die Festlegung europäischer Zertifizierungssysteme für die Cybersicherheit, mit dem für IKT-Produkte, **Prozesse** und Dienste in der Union ein angemessenes Maß an Cybersicherheit gewährleistet werden soll. Dieser Rahmen gilt unbeschadet der in anderen Rechtsakten der Union festgelegten Bestimmungen in Bezug auf eine freiwillige oder verbindliche Zertifizierung.

(Dieser Änderungsantrag betrifft den gesamten Text. Seine Annahme würde entsprechende Abänderungen im gesamten Text erforderlich machen.)

Or. en

Änderungsantrag 130
Jiří Maštálka

Vorschlag für eine Verordnung
Artikel 1 – Absatz 1 – Buchstabe b

Vorschlag der Kommission

(b) ein Rahmen für die Festlegung europäischer Zertifizierungssysteme für die Cybersicherheit, mit dem für IKT-Produkte und Dienste in der Union ein angemessenes Maß an Cybersicherheit gewährleistet werden soll. Dieser Rahmen gilt unbeschadet der in anderen Rechtsakten der Union festgelegten Bestimmungen in Bezug auf eine freiwillige oder verbindliche Zertifizierung.

Geänderter Text

(b) ein Rahmen für die Festlegung europäischer Zertifizierungssysteme für die Cybersicherheit, mit dem für IKT-Produkte, **Prozesse** und Dienste in der Union ein angemessenes Maß an Cybersicherheit gewährleistet werden soll. Dieser Rahmen gilt unbeschadet der in anderen Rechtsakten der Union festgelegten Bestimmungen in Bezug auf eine freiwillige oder verbindliche Zertifizierung.

Or. en

Begründung

Cybersicherheit ist ein bewegliches Ziel, die Zertifizierung des Prozesses, wie des kompletten Lebenszyklus eines Produkts, muss daher in den Anwendungsbereich dieser Verordnung aufgenommen werden.

Änderungsantrag 131

Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung

Artikel 1 – Absatz 1 – Buchstabe b

Vorschlag der Kommission

(b) ein Rahmen für die Festlegung europäischer Zertifizierungssysteme für die Cybersicherheit, mit dem für IKT-Produkte **und** Dienste in der Union ein angemessenes Maß an Cybersicherheit gewährleistet werden soll. Dieser Rahmen gilt unbeschadet der in anderen Rechtsakten der Union festgelegten Bestimmungen in Bezug auf eine **freiwillige oder verbindliche** Zertifizierung.

Geänderter Text

(b) ein Rahmen für die Festlegung europäischer Zertifizierungssysteme für die Cybersicherheit, mit dem für IKT-Produkte, Dienste **und Prozesse** in der Union ein angemessenes Maß an Cybersicherheit gewährleistet werden soll. Dieser Rahmen gilt unbeschadet der in anderen Rechtsakten der Union festgelegten Bestimmungen in Bezug auf Zertifizierung.

Or. en

Änderungsantrag 132

Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung

Artikel 2 – Absatz 1 – Ziffer 1 a (neu)

Vorschlag der Kommission

Geänderter Text

(1a) „Cyberhygiene“ bezeichnet einfache etablierte Routinemaßnahmen wie Multi-Faktor-Authentifizierung, Fehlerkorrektur, Verschlüsselung und Zugriffsmanagement, die Endnutzer ergreifen können, um die Risiken von Cyberbedrohungen auf ein Minimum zu reduzieren;

Änderungsantrag 133

Eva Maydell

Vorschlag für eine Verordnung

Artikel 2 – Absatz 1 – Ziffer 8 a (neu)

Vorschlag der Kommission

Geänderter Text

(8a) „Cyberhygiene“ bezeichnet das Aufstellen von Routinemaßnahmen, die Endnutzer und Unternehmen ergreifen können, um die Risiken von Cyberbedrohungen auf ein Minimum zu reduzieren und sich zu schützen, wenn sie online sind;

Or. en

Änderungsantrag 134

Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung

Artikel 2 – Absatz 1 – Ziffer 9

Vorschlag der Kommission

Geänderter Text

(9) „europäisches System für die Cybersicherheitszertifizierung“ bezeichnet ein umfassendes, auf Unionsebene festgelegtes Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren für die Zertifizierung von Produkten und Diensten der Informations- und Kommunikationstechnik (IKT), die von diesem System erfasst werden;

(9) „europäisches System für die Cybersicherheitszertifizierung“ bezeichnet ein umfassendes, auf Unionsebene festgelegtes Paket von Vorschriften, technischen Anforderungen, Normen **im Einklang mit der Verordnung (EU) 2012/1025**, und Verfahren für die Zertifizierung von Produkten, Diensten **und Prozessen** der Informations- und Kommunikationstechnik (IKT), die von diesem System erfasst werden;

Or. en

Änderungsantrag 135

Roberta Metsola, Eva Maydell, Lara Comi, Pascal Arimont, Antonio López-Istúriz White, Carlos Coelho

Vorschlag für eine Verordnung
Artikel 2 – Absatz 1 – Ziffer 9

Vorschlag der Kommission

(9) „europäisches System für die Cybersicherheitszertifizierung“ bezeichnet ein umfassendes, auf Unionsebene festgelegtes Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren für die Zertifizierung von Produkten und Diensten der Informations- und Kommunikationstechnik (IKT), die von diesem System erfasst werden;

Geänderter Text

(9) „europäisches System für die Cybersicherheitszertifizierung“ bezeichnet ein umfassendes, auf Unionsebene festgelegtes Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren für die Zertifizierung von **Hardware- und Software-**Produkten und Diensten der Informations- und Kommunikationstechnik (IKT), die von diesem System erfasst werden;

Or. en

Änderungsantrag 136
Anneleen Van Bossuyt, Daniel Dalton

Vorschlag für eine Verordnung
Artikel 2 – Absatz 1 – Ziffer 9

Vorschlag der Kommission

(9) „europäisches System für die Cybersicherheitszertifizierung“ bezeichnet ein umfassendes, auf Unionsebene festgelegtes Paket von Vorschriften, **technischen Anforderungen**, Normen und Verfahren für die Zertifizierung von Produkten und Diensten der Informations- und Kommunikationstechnik (IKT), die von diesem System erfasst werden;

Geänderter Text

(9) „europäisches System für die Cybersicherheitszertifizierung“ bezeichnet ein umfassendes, auf Unionsebene festgelegtes Paket von Vorschriften, Normen und Verfahren für die Zertifizierung von Produkten und Diensten der Informations- und Kommunikationstechnik (IKT), die von diesem System erfasst werden;

Or. en

Änderungsantrag 137
Eva Maydell

Vorschlag für eine Verordnung

Artikel 2 – Absatz 1 – Ziffer 10

Vorschlag der Kommission

(10) „europäisches Cybersicherheitszertifikat“ bezeichnet ein von einer Konformitätsbewertungsstelle ausgestelltes Dokument, in dem bescheinigt wird, dass ein bestimmtes IKT-Produkt oder ein bestimmter IKT-Dienst die in einem europäischen System für die Cybersicherheitszertifizierung festgelegten besonderen Anforderungen erfüllt;

Geänderter Text

(10) „europäisches Cybersicherheitszertifikat“ bezeichnet ein von einer Konformitätsbewertungsstelle ausgestelltes Dokument, in dem bescheinigt wird, dass ein bestimmtes IKT-Produkt *oder -System* oder ein bestimmter IKT-Dienst *oder -Prozess* die in einem europäischen System für die Cybersicherheitszertifizierung festgelegten besonderen Anforderungen erfüllt;

Or. en

Änderungsantrag 138

Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová

Vorschlag für eine Verordnung

Artikel 2 – Absatz 1 – Ziffer 10

Vorschlag der Kommission

(10) „europäisches Cybersicherheitszertifikat“ bezeichnet ein von einer Konformitätsbewertungsstelle ausgestelltes Dokument, in dem bescheinigt wird, dass ein bestimmtes IKT-Produkt oder ein bestimmter IKT-Dienst die in einem europäischen System für die Cybersicherheitszertifizierung festgelegten besonderen Anforderungen erfüllt;

Geänderter Text

(10) „europäisches Cybersicherheitszertifikat“ bezeichnet ein von einer Konformitätsbewertungsstelle ausgestelltes Dokument, in dem bescheinigt wird, dass ein bestimmtes IKT-Produkt oder ein bestimmter IKT-Dienst *oder -Prozess* die in einem europäischen System für die Cybersicherheitszertifizierung festgelegten besonderen Anforderungen erfüllt;

Or. en

Begründung

Dieser Änderungsantrag betrifft den gesamten Text. Seine Annahme würde entsprechende Abänderungen im gesamten Text erforderlich machen.

Änderungsantrag 139

Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Artikel 2 – Absatz 1 – Ziffer 10

Vorschlag der Kommission

(10) „europäisches Cybersicherheitszertifikat“ bezeichnet ein von einer Konformitätsbewertungsstelle ausgestelltes Dokument, in dem bescheinigt wird, dass ein bestimmtes IKT-Produkt **oder** ein bestimmter IKT-Dienst die in einem europäischen System für die Cybersicherheitszertifizierung festgelegten besonderen Anforderungen erfüllt;

Geänderter Text

(10) „europäisches Cybersicherheitszertifikat“ bezeichnet ein von einer Konformitätsbewertungsstelle ausgestelltes Dokument, in dem bescheinigt wird, dass ein bestimmtes IKT-Produkt, ein bestimmter IKT-Dienst **oder - Prozess** die in einem europäischen System für die Cybersicherheitszertifizierung festgelegten besonderen Anforderungen erfüllt;

Or. en

Änderungsantrag 140
Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung
Artikel 2 – Absatz 1 – Ziffer 11 a (neu)

Vorschlag der Kommission

Geänderter Text

(11a) „nationale Aufsichtsbehörde für die Zertifizierung“ bezeichnet eine Behörde eines Mitgliedstaats, die für die Kontrolle, Durchsetzung und Aufsicht im Hinblick auf die IT-Sicherheitszertifizierung in ihrem Hoheitsgebiet zuständig ist;

Or. en

Begründung

Der Begriff wurde in dem Text verwendet, ohne dass es für ihn eine klare Begriffsbestimmung gab.

Änderungsantrag 141
Eva Maydell

Vorschlag für eine Verordnung
Artikel 2 – Absatz 1 – Ziffer 11 a (neu)

Vorschlag der Kommission

Geänderter Text

(11a) „IKT-Prozess und -System“ bezeichnet eine Reihe von Verfahren, die in die Entwicklung, den Einsatz und die Pflege von IKT-Produkten und -Diensten integriert sind;

Or. en

Änderungsantrag 142
Jiří Maštálka

Vorschlag für eine Verordnung
Artikel 2 – Absatz 1 – Ziffer 15

Vorschlag der Kommission

Geänderter Text

(15) „Konformitätsbewertungsstelle“ bezeichnet eine Konformitätsbewertungsstelle im Sinne von Artikel 2 Nummer 13 der Verordnung (EG) Nr. 765/2008;

(15) „Konformitätsbewertungsstelle“ bezeichnet eine Konformitätsbewertungsstelle *eines Mitgliedstaats* im Sinne von Artikel 2 Nummer 13 der Verordnung (EG) Nr. 765/2008, *die Konformitätsbewertungstätigkeiten wie Kalibrierung, Tests, Zertifizierung und Überprüfung vornimmt;*

Or. en

Änderungsantrag 143
Roberta Metsola, Lara Comi, Antonio López-Istúriz White, Jiří Pospíšil

Vorschlag für eine Verordnung
Artikel 2 – Absatz 1 – Ziffer 16 a (neu)

Vorschlag der Kommission

Geänderter Text

(16a) „Konformitäts-Eigenerklärung“ bezeichnet die Erklärung eines Herstellers, dass sein IKT-Produkt oder -

Dienst mit den einschlägigen europäischen Systemen für die Cybersicherheitszertifizierung im Einklang steht.

Or. en

Änderungsantrag 144
Andreas Schwab

Vorschlag für eine Verordnung
Artikel 2 – Absatz 1 – Ziffer 16 a (neu)

Vorschlag der Kommission

Geänderter Text

(16a) „Konformitäts-Eigenerklärung“ bezeichnet die Erklärung, durch die der Hersteller dokumentiert, dass für ein Produkt oder einen Dienst bestimmte Anforderungen erfüllt werden.

Or. en

Änderungsantrag 145
Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung
Titel II

Vorschlag der Kommission

Geänderter Text

ENISA – die „**EU-Cybersicherheitsagentur**“

ENISA – die **Agentur der Europäischen Union für Netz- und Informationssicherheit**

Or. en

Begründung

Im Einklang mit dem Vorschlag, die ursprüngliche Bezeichnung der ENISA (Agentur der Europäischen Union für Netz- und Informationssicherheit) beizubehalten.

Änderungsantrag 146
Maria Grapini

Vorschlag für eine Verordnung
Artikel 3 – Absatz 1

Vorschlag der Kommission

1. Die Agentur nimmt die ihr mit dieser Verordnung zugewiesenen Aufgaben mit dem Ziel wahr, zu einem hohen Maß an **Cybersicherheit** innerhalb der Union beizutragen.

Geänderter Text

1. Die Agentur nimmt die ihr mit dieser Verordnung zugewiesenen Aufgaben mit dem Ziel wahr, zu einem hohen Maß an **Informationssicherheit und zur Abwehr von Cyberangriffen** innerhalb der Union beizutragen.

Or. ro

Änderungsantrag 147
Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung
Artikel 3 – Absatz 1

Vorschlag der Kommission

1. Die Agentur nimmt die ihr mit dieser Verordnung zugewiesenen Aufgaben mit dem Ziel wahr, **zu einem hohen** Maß an Cybersicherheit innerhalb der Union **beizutragen**.

Geänderter Text

1. Die Agentur nimmt die ihr mit dieser Verordnung zugewiesenen Aufgaben mit dem Ziel wahr, **ein hohes** Maß an Cybersicherheit innerhalb der Union **zu erreichen**.

Or. en

Begründung

Mit der Änderung werden die Erwartungen im Einklang mit der Tragweite des Vorschlags höher gesetzt.

Änderungsantrag 148
Maria Grapini

Vorschlag für eine Verordnung
Artikel 3 – Absatz 2

Vorschlag der Kommission

2. Die Agentur nimmt die Aufgaben wahr, die ihr durch Rechtsakte der Union übertragen wurden, mit denen die Rechts- und Verwaltungsvorschriften der Mitgliedstaaten auf dem Gebiet der **Cybersicherheit** angeglichen werden sollen.

Geänderter Text

2. Die Agentur nimmt die Aufgaben wahr, die ihr durch Rechtsakte der Union übertragen wurden, mit denen die Rechts- und Verwaltungsvorschriften der Mitgliedstaaten auf dem Gebiet der **Informationssicherheit** angeglichen werden sollen.

Or. ro

Änderungsantrag 149

Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová

**Vorschlag für eine Verordnung
Artikel 3 – Absatz 2 a (neu)**

Vorschlag der Kommission

Geänderter Text

2a. Die Agentur unterstützt die Mitgliedstaaten und die Organe der Union dabei, Strategien und Verfahren für den verantwortlichen Umgang mit nicht öffentlich bekannten Schwachstellen in IKT-Produkten und -Diensten und die koordinierte Offenlegung dieser Schwachstellen aufzustellen.

Or. en

Begründung

Diese Strategien sollten mit den Richtlinien und Empfehlungen in den internationalen Normen ISO/IEC 29147:2014 und ISO/IEC 30111 kohärent sein.

Änderungsantrag 150

Jan Philipp Albrecht

im Namen der Verts/ALE-Fraktion

**Vorschlag für eine Verordnung
Artikel 3 – Absatz 3**

Vorschlag der Kommission

Geänderter Text

3. Von den Zielen und Aufgaben der Agentur unberührt bleiben die Zuständigkeiten der Mitgliedstaaten im Bereich der ***Cybersicherheit sowie auf jeden Fall Tätigkeiten in Bezug auf die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das staatliche Handeln im strafrechtlichen Bereich.***

3. Von den Zielen und Aufgaben der Agenturen unberührt bleiben die ***ausschließlichen*** Zuständigkeiten der Mitgliedstaaten im Bereich der ***IT-Sicherheit.***

Or. en

Begründung

Die aus den Verträgen resultierenden Einschränkungen sollten nicht erweitert werden.

Änderungsantrag 151
Maria Grapini

Vorschlag für eine Verordnung
Artikel 4 – Absatz 2

Vorschlag der Kommission

Geänderter Text

2. Die Agentur unterstützt die Organe, Einrichtungen und sonstigen Stellen der Union sowie die Mitgliedstaaten bei der Ausarbeitung und Umsetzung von Strategien im Zusammenhang mit der ***Cybersicherheit.***

2. Die Agentur unterstützt die Organe, Einrichtungen und sonstigen Stellen der Union sowie die Mitgliedstaaten bei der Ausarbeitung und Umsetzung von Strategien im Zusammenhang mit der ***Informationssicherheit, um Cyberangriffe zu verhindern.***

Or. ro

Änderungsantrag 152
Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung
Artikel 4 – Absatz 4

Vorschlag der Kommission

Geänderter Text

4. Die Agentur fördert auf Unionsebene die Zusammenarbeit und Koordinierung zwischen den Mitgliedstaaten, den Organen, Einrichtungen und sonstigen Stellen der Union sowie den einschlägigen Interessenträgern, auch des Privatsektors, in Fragen, die im Zusammenhang mit der **Cybersicherheit** stehen.

4. Die Agentur fördert auf Unionsebene die Zusammenarbeit und Koordinierung zwischen den Mitgliedstaaten, den Organen, Einrichtungen und sonstigen Stellen der Union sowie den einschlägigen Interessenträgern, auch des Privatsektors, **der Verbraucherschutzverbände und anderer zivilgesellschaftlicher Organisationen**, in Fragen, die im Zusammenhang mit der **IT-Sicherheit** stehen.

Or. en

Begründung

Der Verweis auf den Privatsektor muss auf andere wichtige Interessenträger erweitert werden, insbesondere da die Verbraucher am meisten betroffen sind.

Änderungsantrag 153

Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung

Artikel 4 – Absatz 6

Vorschlag der Kommission

6. Die Agentur fördert die Nutzung der Zertifizierung, **auch indem sie** zum Aufbau und zur Pflege eines Cybersicherheitszertifizierungsrahmens auf Unionsebene **im Sinne des Titels III dieser Verordnung beiträgt**, um die auf mehr Transparenz gestützte Vertrauenswürdigkeit der Cybersicherheit von IKT-Produkten und -Diensten zu erhöhen und damit das Vertrauen in den digitalen Binnenmarkt zu stärken.

Geänderter Text

6. Die Agentur fördert die Nutzung der Zertifizierung, **während sie die Fragmentierung vermeidet, die durch einen Mangel an Koordinierung zwischen vorhandenen Zertifizierungssystemen in der Union entsteht. Die Agentur trägt** zum Aufbau und zur Pflege eines Cybersicherheitszertifizierungsrahmens auf Unionsebene **gemäß der Artikel 43 bis 54 [Titel III] bei**, um die auf mehr Transparenz gestützte Vertrauenswürdigkeit der Cybersicherheit von IKT-Produkten und -Diensten zu erhöhen und damit das Vertrauen in den digitalen Binnenmarkt zu stärken.

Or. en

Änderungsantrag 154
Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Artikel 4 – Absatz 7

Vorschlag der Kommission

7. Die Agentur fördert ein hohes Problembewusstsein der Bürger und Unternehmen in Fragen der Cybersicherheit.

Geänderter Text

7. Die Agentur fördert **ein hohes Maß an Cyberhygiene und** ein hohes Problembewusstsein der Bürger und Unternehmen in Fragen der Cybersicherheit.

Or. en

Änderungsantrag 155
Philippe Juvin

Vorschlag für eine Verordnung
Artikel 4 – Absatz 7

Vorschlag der Kommission

7. Die Agentur fördert ein hohes Problembewusstsein der Bürger und Unternehmen in Fragen der Cybersicherheit.

Geänderter Text

7. Die Agentur fördert **einen hohen Informationsstand und** ein hohes Problembewusstsein der Bürger und Unternehmen in Fragen der Cybersicherheit.

Or. fr

Änderungsantrag 156
Evelyne Gebhardt, Sergio Gutiérrez Prieto, Kerstin Westphal, Lucy Anderson, Arndt Kohn, Catherine Stihler, Marc Tarabella, Pina Picierno, Christel Schaldemose

Vorschlag für eine Verordnung
Artikel 4 – Absatz 7

Vorschlag der Kommission

7. Die Agentur fördert ein hohes Problembewusstsein der Bürger und Unternehmen in Fragen der Cybersicherheit.

Geänderter Text

7. Die Agentur fördert ein hohes Problembewusstsein der Bürger, **Behörden** und Unternehmen in Fragen der Cybersicherheit.

Änderungsantrag 157

Dita Charanzová

Vorschlag für eine Verordnung

Artikel 4 – Absatz 7 a (neu)

Vorschlag der Kommission

Geänderter Text

7a. Die Agentur unterstützt und berät die Mitgliedstaaten und die Organe der Union bei der Aufstellung von Strategien und Verfahren zur Förderung des verantwortlichen Umgangs mit nicht öffentlich bekannten Schwachstellen in IKT-Produkten und -Diensten und die koordinierte Offenlegung dieser Schwachstellen, z. B. Erstellung von Überprüfungsverfahren für die Offenlegung von Schwachstellen in staatlichen Systemen und Richtlinien für die koordinierte Offenlegung von Schwachstellen.

Or. en

Änderungsantrag 158

Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová

Vorschlag für eine Verordnung

Artikel 4 – Absatz 7 a (neu)

Vorschlag der Kommission

Geänderter Text

7a. Die Agentur unterstützt und berät die Mitgliedstaaten und die Organe der Union dabei, Strategien und Verfahren für den verantwortlichen Umgang mit nicht öffentlich bekannten Schwachstellen in IKT-Produkten und -Diensten und die koordinierte Offenlegung dieser Schwachstellen aufzustellen, unter anderem durch die Erstellung von Überprüfungsverfahren

***für die Offenlegung von Schwachstellen
in staatlichen Systemen und Richtlinien
für die koordinierte Offenlegung von
Schwachstellen.***

Or. en

Begründung

Diese Aufgabe sollte im Einklang mit den Richtlinien und Empfehlungen in den internationalen Normen ISO/IEC 29147:2014 und ISO/IEC 30111 ausgeführt werden.

Änderungsantrag 159

Evelyne Gebhardt, Sergio Gutiérrez Prieto, Kerstin Westphal, Lucy Anderson, Arndt Kohn, Pina Picierno

Vorschlag für eine Verordnung

Artikel 5 – Absatz 1 – Ziffer 1

Vorschlag der Kommission

1. ***insbesondere durch unabhängige Stellungnahmen und durch vorbereitende Arbeiten*** zur Ausarbeitung und Überprüfung der Unionspolitik und des Unionsrechts auf dem Gebiet der Cybersicherheit Beratung und Unterstützung gewährt und indem sie sektorspezifische Strategien und Rechtsetzungsinitiativen im Bereich der Cybersicherheit vorlegt;

Geänderter Text

1. zur Ausarbeitung und Überprüfung der Unionspolitik und des Unionsrechts auf dem Gebiet der Cybersicherheit Beratung und Unterstützung gewährt und indem sie sektorspezifische Strategien und Rechtsetzungsinitiativen im Bereich der Cybersicherheit vorlegt;

Or. en

Begründung

Die Agentur sollte bei der Erfüllung ihrer Aufgaben ihre Instrumente frei wählen können.

Änderungsantrag 160

Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová

Vorschlag für eine Verordnung

Artikel 5 – Absatz 1 – Ziffer 2

Vorschlag der Kommission

Geänderter Text

2. die Mitgliedstaaten darin unterstützt, die Unionspolitik und das Unionsrecht auf dem Gebiet der Cybersicherheit, vor allem im Zusammenhang mit der Richtlinie (EU) 2016/1148, kohärent umzusetzen, auch durch Stellungnahmen, Leitlinien, Beratung und bewährte Verfahren zu Themen wie Risikomanagement, Meldung von Sicherheitsvorfällen und Informationsweitergabe, und indem sie den Austausch bewährter Verfahren in diesem Bereich zwischen den zuständigen Behörden erleichtert;

2. die Mitgliedstaaten darin unterstützt, die Unionspolitik und das Unionsrecht auf dem Gebiet der Cybersicherheit, vor allem im Zusammenhang mit der Richtlinie (EU) 2016/1148, kohärent umzusetzen, auch durch Stellungnahmen, Leitlinien, Beratung und bewährte Verfahren zu Themen wie Risikomanagement, Meldung von Sicherheitsvorfällen und Informationsweitergabe, **technische und organisatorische Maßnahmen, insbesondere die Aufstellung von Programmen zur koordinierten Offenlegung von Schwachstellen**, und indem sie den Austausch bewährter Verfahren in diesem Bereich zwischen den zuständigen Behörden erleichtert;

Or. en

Begründung

The NIS-Directive leaves open the range of measures a company can take in order to ensure compliance as part of the “technical and organisational measures” prescribed in Article 14 of Directive (EU) 2016/1148. These measures can include the establishment of a coordinated vulnerability programme, and Member states may explicitly consider parameters regarding the establishment of such a programme in transposing the NIS Directive. ENISA can provide guidelines on how to create such a CVD-programme in order to create a consistent European approach to coordinated vulnerability disclosure that is consistent with the guidelines and recommendations defined in international standards ISO/IEC 29147:2014 and ISO/IEC 30111.

Änderungsantrag 161
Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung
Artikel 5 – Absatz 1 – Ziffer 2 a (neu)

Vorschlag der Kommission

Geänderter Text

2a. den durch die Verordnung (EU) Nr. 2016/679 eingerichteten Europäischen Datenschutzausschuss bei

der Ausarbeitung von Leitlinien unterstützt, in denen auf technischer Ebene die Voraussetzungen angegeben werden, unter denen eine legitime Nutzung personenbezogener Daten durch die Verantwortlichen zu IT-Sicherheitszwecken zulässig ist, um die Infrastruktur zu schützen, indem Angriffe gegen die Informationssysteme aufgedeckt und abgewehrt werden, wobei folgende Vorschriften zu berücksichtigen sind: i) Verordnung (EU) Nr. 2016/679^{1a}; ii) Richtlinie (EU) 2016/1148^{1b}; und iii) Richtlinie 2002/58/EG^{1c};

^{1a} Verordnung (EU) Nr. 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).

^{1b} (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).

^{1c} 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).

Or. en

Begründung

Aufstellung geeigneter Mechanismen zur Kooperation.

Änderungsantrag 162

Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová

Vorschlag für eine Verordnung

Artikel 5 – Absatz 1 – Ziffer 2 a (neu)

Vorschlag der Kommission

Geänderter Text

2a. einen Konzeptentwurf vorschlägt, in dem die Rollen, Verantwortlichkeiten und die gesetzlichen Rechte und Pflichten von Forschern, Verkäufern und Herstellern im Bereich Informationssicherheit, CERTs und CSIRTs in einem Programm zur koordinierten Offenlegung von Schwachstellen festgelegt werden, insbesondere im Falle von Offenlegungen von Schwachstellen, die mehrere Parteien und mehrere Entdecker von Schwachstellen und Verkäufer in verschiedenen Mitgliedstaaten betreffen;

Or. en

Begründung

Die von „Meltdown“ und „Spectre“ ausgenutzten Schwachstellen haben gezeigt, dass es einen Bedarf an unionsweiten Programmen zur Offenlegung von Schwachstellen gibt, deren Anwendungsbereich über die Betreiber wesentlicher Dienste hinausgeht. Dieser Konzeptentwurf sollte mit den in ISO/IEC 29147:2014 und ISO/IEC 30111 festgelegten Richtlinien und Empfehlungen kohärent sein.

Änderungsantrag 163

Jan Philipp Albrecht

im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung

Artikel 5 – Absatz 1 – Nummer 2 b (neu)

Vorschlag der Kommission

Geänderter Text

2b. Leitlinien vorschlägt, mit denen sichergestellt werden soll, dass die IKT-Hersteller ihre Sorgfaltspflicht erfüllen,

wenn es darum geht, IT-Sicherheitslücken in ihren Produkten und Dienstleistungen rasch zu beseitigen, damit ihre Nutzer nicht über Gebühr der Gefahr von Computerkriminalität ausgesetzt sind;

Or. en

Begründung

Die Verantwortlichkeiten müssen genau analysiert werden, um alle Interessenträger dazu zu ermutigen, ihrer Sorgfaltspflicht nachzukommen.

Änderungsantrag 164

Jan Philipp Albrecht

im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung

Artikel 5 – Absatz 1 – Nummer 2 c (neu)

Vorschlag der Kommission

Geänderter Text

2c. Leitlinien vorschlagen, mit denen ein robuster Rahmen für die Verantwortlichkeiten und Haftungspflichten sämtlicher Interessenträger der IKT-Ökosysteme entwickelt wird;

Or. en

Begründung

Ermütigung aller Interessenträger, umsichtig zu handeln.

Änderungsantrag 165

Jan Philipp Albrecht

im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung

Artikel 5 – Absatz 1 – Nummer 2 d (neu)

Vorschlag der Kommission

Geänderter Text

2d. Leitlinien vorschlägt, die eine Verschärfung der Vorschriften für die Verantwortlichkeiten der Betreiber kritischer Netzinfrastrukturen bei einem Angriff auf ihre Informationssysteme betreffen, der sich aufgrund mangelnder Sorgfalt seitens einiger Nutzer oder des Betreibers selbst nachteilig auf die Nutzer auswirkt, sofern es der Betreiber versäumt hat, gebotene Vorkehrungen zur Verhütung des Vorfalls oder zur Abmilderung der Folgen auf alle Nutzer zu treffen;

Or. en

Begründung

Die Betreiber kritischer Infrastrukturen sollten in gewissem Maße sicherstellen müssen, dass nur sichere und vertrauenswürdige Nutzer/Anwender ihre Infrastruktur nutzen. Gegebenenfalls sollten sie nicht sichere Nutzer isolieren, um Vorfälle zu vermeiden.

Änderungsantrag 166
Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung
Artikel 5 – Absatz 1 – Nummer 2 e (neu)

Vorschlag der Kommission

Geänderter Text

2e. Leitlinien vorschlägt, mit denen der Erwerb und der Einsatz von „Zero-Days“ durch Behörden für Angriffe auf Informationssysteme beschränkt wird; Software-Prüfungen fördert und Fachpersonal finanziert;

Or. en

Begründung

Wenn staatliche Stellen mit Steuergeldern Hintertüren für IT-Systeme entwickeln, erwerben oder ausnutzen, setzen sie dabei die Sicherheit der Bürger aufs Spiel. Damit andere Interessenträger, die verantwortlich mit solchen Schwachstellen umgehen, geschützt werden, sollte die Agentur Maßnahmen dazu vorschlagen, wie Informationen zu „Zero-Days“ und zu anderen noch nicht allgemein bekannten Sicherheitslücken auf verantwortungsvolle Weise

ausgetauscht werden können, zumal diese Maßnahmen die Beseitigung dieser Schwachstellen erleichtern würden.

Änderungsantrag 167

Jan Philipp Albrecht

im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung

Artikel 5 – Absatz 1 – Nummer 2 f (neu)

Vorschlag der Kommission

Geänderter Text

2f. Leitlinien für Behörden, private Unternehmen, Forscher, Universitäten und andere Interessenträger vorschlägt, die die Veröffentlichung sämtlicher noch nicht allgemein bekannter kritischer Sicherheitslücken im Rahmen einer verantwortungsvollen Offenlegung betreffen;

Or. en

Begründung

Für die Einführung einheitlicher, verantwortungsvoller Offenlegungsverfahren in der gesamten EU werden geeignete politische Strategien auf der Ebene der EU benötigt.

Änderungsantrag 168

Jan Philipp Albrecht

im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung

Artikel 5 – Absatz 1 – Nummer 2 g (neu)

Vorschlag der Kommission

Geänderter Text

2g. Leitlinien vorschlägt, die darauf abzielen, die Verwendung überprüfbarer, quelloffener Codes für IT-Lösungen im öffentlichen Sektor auszuweiten und damit verbundene automatisierte Instrumente einzusetzen, um die Prüfung von Quellcodes zu erleichtern und um problemlos zu überprüfen, dass es keine Hintertüren oder etwaige andere

Sicherheitslücken gibt;

Or. en

Begründung

Die Verwendung quelloffener Software in öffentlichen Verwaltungen sollte gefördert werden, wobei diese aber auch die Verantwortung dafür übernehmen sollten, den Quellcode der von ihnen verwendeten Anwendungen (auf etwaige größere IT-Sicherheitslücken) zu überprüfen.

Änderungsantrag 169

Evelyne Gebhardt, Sergio Gutiérrez Prieto, Kerstin Westphal, Lucy Anderson, Arndt Kohn, Marc Tarabella, Pina Picierno, Christel Schaldemose

Vorschlag für eine Verordnung

Artikel 5 – Absatz 1 – Nummer 4 – Ziffer 2

Vorschlag der Kommission

(2) die Förderung eines höheren Sicherheitsniveaus in der elektronischen Kommunikation, auch indem sie ihre Sachkenntnis und Beratung anbietet und den Austausch bewährter Verfahren zwischen den zuständigen Behörden erleichtert;

Geänderter Text

(2) die Förderung eines höheren Sicherheitsniveaus in der elektronischen Kommunikation, ***der Speicherung und Verarbeitung von Daten***, auch indem sie ihre Sachkenntnis und Beratung anbietet und den Austausch bewährter Verfahren zwischen den zuständigen Behörden erleichtert;

Or. en

Änderungsantrag 170

Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová

Vorschlag für eine Verordnung

Artikel 5 – Absatz 1 – Nummer 4 – Ziffer 2 a (neu)

Vorschlag der Kommission

Geänderter Text

(2a) die Entwicklung und Förderung von Strategien, die die allgemeine Verfügbarkeit oder Integrität des öffentlichen Kerns des offenen Internets bewahren, der die wesentlichen Funktionen des Internets insgesamt bereitstellt und seinen normalen Betrieb

stützt, darunter u. a. die Sicherheit und Stabilität der wichtigsten Protokolle (insbesondere DNS, BGP und IPv6), den Betrieb des Domain Name Systems (einschließlich aller Top-Level-Domains) und den Betrieb der Rootzone;

Or. en

Begründung

Der Schutz des öffentlichen Kerns des Internets ist eine neu entstehende Norm, die von der Global Commission on the Stability for Cyberspace unterstützt wird, die ihr Mandat aus den Schlussakten der 4. Global Conference on CyberSpace (GCCS), die 2015 in Den Haag stattfand, sowie aus dem 5. Bericht der VN-Gruppe von Regierungssachverständigen erhalten hat.

Änderungsantrag 171

Eva Maydell

Vorschlag für eine Verordnung

Artikel 6 – Absatz 1 – Buchstabe a

Vorschlag der Kommission

(a) die Mitgliedstaaten bei ihren Bemühungen zur Verhütung, Erkennung und Analyse und zur Stärkung ihrer Kapazitäten für die Bewältigung von Problemen und Vorfällen im Bereich der Cybersicherheit, indem sie ihnen das erforderliche Wissen und die notwendigen Sachkenntnisse zur Verfügung stellt;

Geänderter Text

(a) die Mitgliedstaaten bei ihren Bemühungen zur Verhütung, Erkennung und Analyse und zur Stärkung ihrer Kapazitäten für die Bewältigung von Problemen und Vorfällen im Bereich der Cybersicherheit, indem sie ihnen das erforderliche Wissen und die notwendigen Sachkenntnisse zur Verfügung stellt, ***inklusive eines vom Personal und von den Bürgern einzuhaltenden Sets an Cyberhygiene-Routinen.***;

Or. en

Änderungsantrag 172

Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová

Vorschlag für eine Verordnung

Artikel 6 – Absatz 1 – Buchstabe a a (neu)

(aa) die Mitgliedstaaten und die Organe der Union bei der Aufstellung und Umsetzung von Strategien für eine koordinierte Offenlegung von Schwachstellen und für einen Überprüfungsprozess für die Offenlegung von Schwachstellen in staatlichen Systemen, deren Verfahren und Bestimmungen transparent sein und einer unabhängigen Überwachung unterliegen sollten;

Or. en

Begründung

Ein Überprüfungsprozess für die Offenlegung von Schwachstellen in staatlichen Systemen umfasst den Umgang mit Schwachstellen, die von staatlichen Stellen entdeckt werden, und legt fest, wann und wie die staatliche Stelle die bei ihr entdeckte Schwachstelle bekanntgeben muss. Es wird sichergestellt, dass Regierungen und ihre Stellen solide Strategien für die Überprüfung und Koordinierung der Offenlegung von Schwachstellen haben. Dies ist eine kritische Norm, die in der EU vorangetrieben werden sollte.

Änderungsantrag 173

Dita Charanzová

Vorschlag für eine Verordnung

Artikel 6 – Absatz 1 – Buchstabe a a (neu)

(aa) die Mitgliedstaaten und die Organe der Union bei der Aufstellung und Umsetzung von Strategien für die koordinierte Offenlegung von Schwachstellen und Prozessen für Schwachstellen in staatlichen Systemen, deren Verfahren und Bestimmungen einer unabhängigen Aufsicht unterliegen und transparent sein müssen;

Or. en

Änderungsantrag 174
Dita Charanzová

Vorschlag für eine Verordnung
Artikel 6 – Absatz 2

Vorschlag der Kommission

2. Die Agentur erleichtert die Einrichtung sektorbezogener Informationsaustausch- und -analysezentren (Information Sharing and Analysis Centres – ISACs) und unterstützt diese dauerhaft, vor allem in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren, indem sie bewährte Verfahren und Leitlinien zu den verfügbaren Instrumenten und Verfahren sowie zur Bewältigung rechtlicher Fragen im Zusammenhang mit der Informationsweitergabe bereitstellt.

Geänderter Text

2. Die Agentur erleichtert die Einrichtung sektorbezogener Informationsaustausch- und -analysezentren (Information Sharing and Analysis Centres – ISACs) und unterstützt diese dauerhaft, vor allem in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren, indem sie bewährte Verfahren und Leitlinien zu den verfügbaren Instrumenten und Verfahren, **Cyberhygiene-Grundsätzen** sowie zur Bewältigung rechtlicher Fragen im Zusammenhang mit der Informationsweitergabe bereitstellt.

Or. en

Änderungsantrag 175
Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

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

Vorschlag der Kommission

Geänderter Text

2a. Die Agentur setzt sich dafür ein, dass ein langfristiges EU-Projekt im Bereich der IT-Sicherheit ausgearbeitet und auf den Weg gebracht wird, mit dem das Wachstum einer unabhängigen IT-Sicherheitsbranche in der EU gefördert wird und der Aspekt der IT-Sicherheit in der EU bei allen Entwicklungen im IT-Bereich Berücksichtigung findet.

Or. en

Begründung

Die ENISA sollte die Gesetzgeber bei der Erstellung von politischen Strategien beraten, die es der EU ermöglichen, den Rückstand zu der IT-Sicherheitsbranche in Drittländern aufzuholen. Das Projekt sollte vom Umfang her mit den Anstrengungen vergleichbar sein, die zugunsten der Luftfahrt (siehe Airbus) unternommen wurden. Für die Schaffung einer stärkeren, unabhängigen und vertrauenswürdigen IKT-Branche in der EU ist dies unabdingbar (siehe Studie des Referats Wissenschaftliche Vorausschau (STOA), PE 614.531).

Änderungsantrag 176

Maria Grapini

Vorschlag für eine Verordnung

Artikel 7 – Absatz 1 – Unterabsatz 1

Vorschlag der Kommission

Auf Ersuchen von **zwei** oder mehreren betroffenen Mitgliedstaaten und zu dem alleinigen Zweck, Beratung im Hinblick auf die Vermeidung künftiger Sicherheitsvorfälle anzubieten, unterstützt die Agentur, nachdem Unternehmen gemäß der Richtlinie (EU) 2016/1148 Sicherheitsvorfälle mit beträchtlichen oder erheblichen Auswirkungen gemeldet hatten, eine technische Ex-post-Untersuchung oder führt diese selbst durch. Eine derartige Untersuchung führt die Agentur auch dann durch, wenn sie bei solchen Sicherheitsvorfällen, von denen mindestens zwei Mitgliedstaaten betroffen sind, von der Kommission im Einvernehmen mit den betroffenen Mitgliedstaaten in einem hinreichend begründeten Ersuchen dazu aufgefordert wurde.

Geänderter Text

Auf Ersuchen von **einem** oder mehreren betroffenen Mitgliedstaaten und zu dem alleinigen Zweck, Beratung im Hinblick auf die Vermeidung künftiger Sicherheitsvorfälle anzubieten, unterstützt die Agentur, nachdem Unternehmen gemäß der Richtlinie (EU) 2016/1148 Sicherheitsvorfälle mit beträchtlichen oder erheblichen Auswirkungen gemeldet hatten, eine technische Ex-post-Untersuchung oder führt diese selbst durch. Eine derartige Untersuchung führt die Agentur auch dann durch, wenn sie bei solchen Sicherheitsvorfällen, von denen mindestens zwei Mitgliedstaaten betroffen sind, von der Kommission im Einvernehmen mit den betroffenen Mitgliedstaaten in einem hinreichend begründeten Ersuchen dazu aufgefordert wurde.

Or. ro

Änderungsantrag 177

Evelyne Gebhardt, Sergio Gutiérrez Prieto, Kerstin Westphal, Lucy Anderson, Arndt Kohn, Catherine Stihler, Marc Tarabella, Pina Picierno, Christel Schaldemose

Vorschlag für eine Verordnung

Artikel 7 – Absatz 8 – Buchstabe a

Vorschlag der Kommission

(a) Berichte aus nationalen Quellen als Beitrag zu einer gemeinsamen Lageerfassung zusammenstellt;

Geänderter Text

(a) Berichte aus nationalen **und internationalen** Quellen als Beitrag zu einer gemeinsamen Lageerfassung zusammenstellt;

Or. en

Änderungsantrag 178

Jan Philipp Albrecht

im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung

Artikel 7 – Absatz 8 – Buchstabe c a (neu)

Vorschlag der Kommission

Geänderter Text

(ca) Zertifizierungssysteme einrichtet, die IKT-Hersteller und -Dienstleister davon abhalten, geheime Hintertüren einzubauen, die die IT-Sicherheit kommerzieller Produkte und Dienstleistungen gezielt schwächen und sich nachteilig auf die allgemeine Sicherheit des Internets auswirken;

Or. en

Begründung

Dies sollte als eines der zentralen Ziele der Zertifizierungssysteme anerkannt werden.

Änderungsantrag 179

Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová

Vorschlag für eine Verordnung

Artikel 7 – Absatz 8 – Buchstabe e a (neu)

Vorschlag der Kommission

Geänderter Text

(ea) die Mitgliedstaaten bei der Aufstellung und Umsetzung von

***Strategien für die koordinierte
Offenlegung von Schwachstellen und für
Überprüfungsprozesse für die
Offenlegung von Schwachstellen in
staatlichen Systemen unterstützt und
berät.***

Or. en

Begründung

Diese Aufgabe sollte im Einklang mit den in den Normen ISO/IEC 29147:2014 und ISO/IEC 30111 festgelegten Richtlinien und Empfehlungen ausgeführt werden.

**Änderungsantrag 180
Antanas Guoga**

**Vorschlag für eine Verordnung
Artikel 8 – Absatz 1 – Buchstabe a– Ziffer 1**

Vorschlag der Kommission

(1) mögliche europäische Systeme für die Cybersicherheitszertifizierung von IKT-Produkten und -Diensten nach Artikel 44 dieser Verordnung ausarbeitet;

Geänderter Text

(1) ***in Absprache mit den Interessenträgern der Branche in einem formalen, standardisierten und transparenten Verfahren*** mögliche europäische Systeme für die Cybersicherheitszertifizierung von IKT-Produkten und -Diensten nach Artikel 44 dieser Verordnung ***ermittelt und*** ausarbeitet;

Or. en

**Änderungsantrag 181
Nicola Danti, Evelyne Gebhardt, Maria Grapini, Sergio Gutiérrez Prieto, Lucy Anderson, Arndt Kohn, Catherine Stihler, Pina Picierno, Marc Tarabella, Christel Schaldemose**

**Vorschlag für eine Verordnung
Artikel 8 – Absatz 1 – Buchstabe a – Ziffer 1 a (neu)**

Vorschlag der Kommission

Geänderter Text

(1a) regelmäßig unabhängige Ex-Post-

***Kontrollen zur Konformität der
zertifizierten IKT-Produkte und -Dienste
mit dieser Richtlinie durchführt;***

Or. en

Begründung

Neben der Überwachung auf Ebene der Mitgliedstaaten muss es eine Überwachung auf EU-Ebene geben, um dafür zu sorgen, dass die Konformität auf koordinierte Weise EU-weit sichergestellt wird.

**Änderungsantrag 182
Dita Charanzová, Morten Løkkegaard**

**Vorschlag für eine Verordnung
Artikel 8 – Absatz 1 – Buchstabe a– Ziffer 3**

Vorschlag der Kommission

(3) in Zusammenarbeit mit nationalen Aufsichtsbehörden für die Zertifizierung Leitlinien zusammenstellt und veröffentlicht sowie bewährte Verfahren im Zusammenhang mit den Anforderungen an die Cybersicherheit von IKT-Produkten und -Diensten entwickelt;

Geänderter Text

(3) in Zusammenarbeit mit nationalen Aufsichtsbehörden für die Zertifizierung ***in einem formalen, standardisierten und transparenten Verfahren*** Leitlinien zusammenstellt und veröffentlicht sowie bewährte Verfahren im Zusammenhang mit den Anforderungen an die Cybersicherheit von IKT-Produkten und -Diensten, ***einschließlich Grundsätzen der Cyberhygiene*** entwickelt;

Or. en

**Änderungsantrag 183
Antanas Guoga**

**Vorschlag für eine Verordnung
Artikel 8 – Absatz 1 – Buchstabe a– Ziffer 3**

Vorschlag der Kommission

(3) in Zusammenarbeit mit nationalen Aufsichtsbehörden für die Zertifizierung Leitlinien zusammenstellt und veröffentlicht sowie bewährte Verfahren

Geänderter Text

(3) in Zusammenarbeit mit nationalen Aufsichtsbehörden für die Zertifizierung ***in einem formalen, standardisierten und transparenten Verfahren*** Leitlinien

im Zusammenhang mit den Anforderungen an die Cybersicherheit von IKT-Produkten und -Diensten entwickelt;

zusammenstellt und veröffentlicht sowie bewährte Verfahren im Zusammenhang mit den Anforderungen an die Cybersicherheit von IKT-Produkten und -Diensten entwickelt;

Or. en

Änderungsantrag 184
Antanas Guoga

Vorschlag für eine Verordnung
Artikel 8 – Absatz 1 – Buchstabe a – Ziffer 3 a (neu)

Vorschlag der Kommission

Geänderter Text

(3a) in Absprache mit allen einschlägigen Interessenträgern ermittelt, ob für einen bestimmten Bedarf nicht bereits irgendwo auf der Welt Standards oder Zertifizierungsprozesse existieren, und falls Lücken festgestellt werden, Organisationen zur Entwicklung von Normen dazu auffordert, Normen oder Verfahren zu entwickeln;

Or. en

Änderungsantrag 185
Anneleen Van Bossuyt, Daniel Dalton

Vorschlag für eine Verordnung
Artikel 8 – Absatz 1 – Buchstabe b

Vorschlag der Kommission

Geänderter Text

(b) erleichtert die Ausarbeitung und Übernahme europäischer und internationaler Normen für das Risikomanagement und die Sicherheit von IKT-Produkten und -Diensten bietet nach Artikel 19 Absatz 2 der Richtlinie (EU) 2016/1148 in Zusammenarbeit mit den Mitgliedstaaten Beratung an und erlässt Leitlinien für die technischen

(b) konsultiert internationale und europäische Normungsgremien bezüglich der Entwicklung von Normen für das Risikomanagement und die Sicherheit von IKT-Produkten und -Diensten und erleichtert die Ausarbeitung und Übernahme sachdienlicher und europäischer Normen;

Bereiche, die sich auf die Sicherheitsanforderungen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste beziehen, sowie für bereits vorhandene Normen, auch nationale Normen der Mitgliedstaaten;

Or. en

Änderungsantrag 186
Antanas Guoga

Vorschlag für eine Verordnung
Artikel 8 – Absatz 1 – Buchstabe b

Vorschlag der Kommission

(b) erleichtert die Ausarbeitung und Übernahme europäischer ***und*** internationaler Normen für das Risikomanagement und die Sicherheit von IKT-Produkten und -Diensten bietet nach Artikel 19 Absatz 2 der Richtlinie (EU) 2016/1148 in Zusammenarbeit mit den Mitgliedstaaten Beratung an und erlässt Leitlinien für die technischen Bereiche, die sich auf die Sicherheitsanforderungen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste beziehen, sowie für bereits vorhandene Normen, auch nationale Normen der Mitgliedstaaten;

Geänderter Text

(b) erleichtert die Ausarbeitung und Übernahme europäischer ***oder*** internationaler Normen für das Risikomanagement und die Sicherheit von IKT-Produkten und -Diensten bietet nach Artikel 19 Absatz 2 der Richtlinie (EU) 2016/1148 in Zusammenarbeit mit den Mitgliedstaaten Beratung an und erlässt Leitlinien für die technischen Bereiche, die sich auf die Sicherheitsanforderungen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste beziehen, sowie für bereits vorhandene Normen, auch nationale Normen der Mitgliedstaaten;

Or. en

Änderungsantrag 187
Anneleen Van Bossuyt, Daniel Dalton

Vorschlag für eine Verordnung
Artikel 8 – Absatz 1 – Buchstabe b a (neu)

Vorschlag der Kommission

Geänderter Text

(ba) bietet in Zusammenarbeit mit den Mitgliedstaaten Beratung und erlässt

Leitlinien zu den technischen Bereichen, die unter Buchstabe b genannt werden, sowie zu den bereits bestehenden Normen — einschließlich der nationalen Normen der Mitgliedstaaten —, mit denen diese Bereiche abgedeckt werden könnten;

Or. en

Änderungsantrag 188
Antanas Guoga

Vorschlag für eine Verordnung
Artikel 8 – Absatz 1 – Buchstabe b a (neu)

Vorschlag der Kommission

Geänderter Text

(ba) setzt in ihrer Arbeit Prioritäten auf die Bestandsaufnahme der auf nationaler Ebene vorhandenen Systeme sowie auf die Entwicklung von Leitlinien für eine mögliche Harmonisierung dieser Systeme, um eine gegenseitige Anerkennung innerhalb der Union zu schaffen;

Or. en

Änderungsantrag 189
Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung
Artikel 8 – Absatz 1 – Buchstabe c a (neu)

Vorschlag der Kommission

Geänderter Text

(ca) richtet Zertifizierungssysteme ein, die IKT-Hersteller und -Dienstleister davon abhalten, geheime Hintertüren einzubauen, die die IT-Sicherheit kommerzieller Produkte und Dienstleistungen gezielt schwächen und sich nachteilig auf die allgemeine Sicherheit des Internets auswirken;

Begründung

Dies sollte als eines der zentralen Ziele der Zertifizierungssysteme anerkannt werden.

Änderungsantrag 190

Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová

Vorschlag für eine Verordnung

Artikel 8 – Absatz 1 – Buchstabe c a (neu)

Vorschlag der Kommission

Geänderter Text

(ca) unterstützt und fördert die Entwicklung und Umsetzung von Richtlinien für die koordinierte Offenlegung von Schwachstellen und für Überprüfungsprozesse für die Offenlegung von Schwachstellen in staatlichen Systemen;

Or. en

Änderungsantrag 191

Liisa Jaakonsaari, Christel Schaldemose, Lucy Anderson

Vorschlag für eine Verordnung

Artikel 9 – Absatz 1 – Buchstabe d

Vorschlag der Kommission

Geänderter Text

(d) bündelt die von den Organen, Einrichtungen und sonstigen Stellen der Union bereitgestellten Informationen zur Cybersicherheit, ordnet diese Informationen und stellt sie über ein eigenes Portal der Öffentlichkeit zur Verfügung;

(d) bündelt die von den Organen, Einrichtungen und sonstigen Stellen der Union bereitgestellten Informationen zur Cybersicherheit, ordnet diese Informationen und stellt sie über ein eigenes Portal der Öffentlichkeit zur Verfügung, ***einschließlich Informationen zu wichtigen Cybersicherheitsvorfällen und größeren Verletzungen des Schutzes personenbezogener Daten sowie Informationen zu Anbietern oder Herstellern, die von der ENISA eine Warnung bezüglich des Maßes an Cybersicherheit ihrer Produkte erhalten***

haben;

Or. en

Änderungsantrag 192

Jiří Pospíšil

Vorschlag für eine Verordnung Artikel 9 – Absatz 1 – Buchstabe d

Vorschlag der Kommission

d) bündelt die von den Organen, Einrichtungen und sonstigen Stellen der Union bereitgestellten Informationen zur Cybersicherheit, ordnet diese Informationen und stellt sie über ein eigenes Portal der Öffentlichkeit zur Verfügung;

Geänderter Text

d) bündelt die von den Organen, Einrichtungen und sonstigen Stellen der Union bereitgestellten Informationen zur Cybersicherheit, ordnet diese Informationen und stellt sie über ein eigenes Portal der Öffentlichkeit zur Verfügung;

Or. cs

Änderungsantrag 193

Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung Artikel 9 – Absatz 1 – Buchstabe e

Vorschlag der Kommission

(e) sensibilisiert die Öffentlichkeit für Cybersicherheitsrisiken und stellt Leitlinien für bewährte Verfahren zur Verfügung, die sich an Bürger und Organisationen wenden;

Geänderter Text

(e) sensibilisiert die Öffentlichkeit für Cybersicherheitsrisiken und stellt Leitlinien für bewährte Verfahren **der Cyberhygiene** zur Verfügung, die sich an Bürger und Organisationen wenden;

Or. en

Änderungsantrag 194

Jan Philipp Albrecht

im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung

Artikel 9 – Absatz 1 – Buchstabe e

Vorschlag der Kommission

(e) sensibilisiert die Öffentlichkeit für Cybersicherheitsrisiken und stellt Leitlinien für bewährte Verfahren zur Verfügung, die sich an Bürger und Organisationen wenden;

Geänderter Text

(Betrifft nicht die deutsche Fassung.)

Or. en

Änderungsantrag 195

Eva Maydell

Vorschlag für eine Verordnung

Artikel 9 – Absatz 1 – Buchstabe e a (neu)

Vorschlag der Kommission

Geänderter Text

(ea) unterstützt eine bessere Kooperation mit den Mitgliedstaaten, um über Cybersicherheit aufzuklären und für das Thema zu sensibilisieren, sowie beim Thema Cyberhygiene;

Or. en

Änderungsantrag 196

Jan Philipp Albrecht

im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung

Artikel 9 – Absatz 1 – Buchstabe g a (neu)

Vorschlag der Kommission

Geänderter Text

(ga) setzt sich dafür an, dass alle Akteure des digitalen Binnenmarkts der EU robuste Präventivmaßnahmen für IT-Sicherheit ergreifen und als erste Verteidigungslinie gegen Angriffe auf Informationssysteme zuverlässige Technologien für den Datenschutz und zum Schutz der Privatsphäre einsetzen;

Begründung

Dies geht auf die Stellungnahme des EDSB (zu Technologie zum Schutz der Privatsphäre) zurück. Das Aufgabenfeld der ENISA sollte eindeutig über die Unterstützung der Mitgliedstaaten, der Kommission und der Agenturen der EU hinausgehen. Zugleich sollte die Agentur aber auch stärker in den Mittelpunkt der Aufmerksamkeit sowohl der Branche als auch der allgemeinen Öffentlichkeit rücken.

Änderungsantrag 197**Dita Charanzová, Morten Løkkegaard****Vorschlag für eine Verordnung****Artikel 9 – Absatz 1 – Buchstabe g a (neu)***Vorschlag der Kommission**Geänderter Text*

(ga) unterstützt eine bessere Koordinierung und den Austausch bewährter Verfahren zwischen den Mitgliedstaaten, wenn es darum geht, über Cybersicherheit und Cyberhygiene aufzuklären und für das Thema zu sensibilisieren, indem ein Netz nationaler Bildungskontaktstellen geschaffen und unterhalten wird.

Or. en

Änderungsantrag 198**Inese Vaidere****Vorschlag für eine Verordnung****Artikel 10 – Absatz 1 – Buchstabe a***Vorschlag der Kommission**Geänderter Text*

(a) berät **die Agentur** die Union und die Mitgliedstaaten zum Forschungsbedarf und zu den Forschungsprioritäten im Bereich der Cybersicherheit, damit die Voraussetzung für wirksame Reaktionen auf die gegenwärtigen oder sich abzeichnenden Risiken und Bedrohungen, auch in Bezug auf neue und aufkommende

(a) **sorgt die Agentur für Vorkonsultationen mit den einschlägigen Nutzergruppen** und berät die Union und die Mitgliedstaaten zum Forschungsbedarf und zu den Forschungsprioritäten im Bereich der Cybersicherheit, damit die Voraussetzung für wirksame Reaktionen auf die gegenwärtigen oder sich

Informations- und Kommunikationstechnik (IKT), geschaffen und die Techniken zur Risikovermeidung genutzt werden können;

abzeichnenden Risiken und Bedrohungen, auch in Bezug auf neue und aufkommende Informations- und Kommunikationstechnik (IKT), geschaffen und die Techniken zur Risikovermeidung genutzt werden können;

Or. en

Änderungsantrag 199

Jan Philipp Albrecht

im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung

Artikel 10 – Absatz 1 – Buchstabe a

Vorschlag der Kommission

(a) berät die Agentur die Union und die Mitgliedstaaten zum Forschungsbedarf und zu den Forschungsprioritäten **im Bereich der** Cybersicherheit, damit die Voraussetzung für wirksame Reaktionen auf die gegenwärtigen oder sich abzeichnenden Risiken und Bedrohungen, auch in Bezug auf neue und aufkommende Informations- und Kommunikationstechnik (IKT), geschaffen und die Techniken zur Risikovermeidung genutzt werden können;

Geänderter Text

(a) berät die Agentur die Union und die Mitgliedstaaten zum Forschungsbedarf und zu den Forschungsprioritäten **in den Bereichen** Cybersicherheit, **Datenschutz und Schutz der Privatsphäre**, damit die Voraussetzung für wirksame Reaktionen auf die gegenwärtigen oder sich abzeichnenden Risiken und Bedrohungen, auch in Bezug auf neue und aufkommende Informations- und Kommunikationstechnik (IKT), geschaffen und die Techniken zur Risikovermeidung genutzt werden können;

Or. en

Begründung

Dies geht auf die Stellungnahme des EDSB zurück. In der vorherigen Verordnung (EU) Nr. 526/2013 war vorgesehen, dass die ENISA Forschungsaufgaben im Bereich Datenschutz und Privatsphäre übernimmt. In dem Vorschlag der Kommission ist dies nicht mehr vorgesehen. Die Streichung der Forschungs- und Beratungsaufgaben wird wahrscheinlich dazu führen, dass die ENISA ihre Arbeiten zu den Technologien zum Schutz der Privatsphäre bzw. zum Datenschutz sowie allgemein zu Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen einstellt.

Änderungsantrag 200

Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Artikel 11 – Absatz 1 – Buchstabe c a (neu)

Vorschlag der Kommission

Geänderter Text

(ca) die multilaterale Zusammenarbeit bei der Regulierung und Normung unterstützt, um faire Wettbewerbsbedingungen zu schaffen, die den Vorgaben der WTO entsprechen.

Or. en

Änderungsantrag 201
Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Artikel 11 – Absatz 1 – Buchstabe c b (neu)

Vorschlag der Kommission

Geänderter Text

(cb) Bemühungen um die Aufnahme von Bestimmungen zur Cybersicherheit in Freihandelsabkommen unterstützt;

Or. en

Änderungsantrag 202
Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung
Artikel 13 – Absatz 1

Vorschlag der Kommission

Geänderter Text

1. Dem Verwaltungsrat gehören je ein Vertreter jedes Mitgliedstaats und zwei von der Kommission ernannte Vertreter an. Alle Vertreter verfügen über Stimmrecht.

1. Dem Verwaltungsrat gehören je ein Vertreter jedes Mitgliedstaats, **drei Vertreter der Ständigen Gruppe der Interessenträger, von denen einer die Interessen der Verbraucher vertreten muss**, und zwei von der Kommission ernannte Vertreter an. Alle Vertreter verfügen über Stimmrecht.

Begründung

Der Vorschlag sollte sicherstellen, dass die Interessen aller Interessenträger in der Organisationsstruktur der ENISA angemessen vertreten sind.

Änderungsantrag 203

Evelyne Gebhardt, Sergio Gutiérrez Prieto, Kerstin Westphal, Lucy Anderson, Arndt Kohn, Marc Tarabella, Pina Picierno, Christel Schaldemose

Vorschlag für eine Verordnung**Artikel 13 – Absatz 1***Vorschlag der Kommission*

1. Dem Verwaltungsrat gehören je ein Vertreter jedes Mitgliedstaats und zwei von der Kommission ernannte Vertreter an. Alle Vertreter verfügen über Stimmrecht.

Geänderter Text

1. Dem Verwaltungsrat gehören je ein Vertreter jedes Mitgliedstaats und zwei von der Kommission **und vom Europäischen Parlament** ernannte Vertreter an. Alle Vertreter verfügen über Stimmrecht.

Or. en

Änderungsantrag 204

Jiří Pospíšil

Vorschlag für eine Verordnung**Artikel 14 – Absatz 1 – Buchstabe e***Vorschlag der Kommission*

(e) bewertet und genehmigt den konsolidierten Jahresbericht über die Tätigkeiten der Agentur und übermittelt den Bericht zusammen mit seiner Bewertung bis zum 1. Juli des folgenden Jahres dem Europäischen Parlament, dem Rat, der Kommission und dem Rechnungshof. Der Jahresbericht enthält den Jahresabschluss **und** Ausführungen **darüber**, inwiefern die Agentur die vorgegebenen Leistungsindikatoren erfüllt hat. Der Jahresbericht wird veröffentlicht;

Geänderter Text

(e) bewertet und genehmigt den konsolidierten Jahresbericht über die Tätigkeiten der Agentur und übermittelt den Bericht zusammen mit seiner Bewertung bis zum 1. Juli des folgenden Jahres dem Europäischen Parlament, dem Rat, der Kommission und dem Rechnungshof. Der Jahresbericht enthält den Jahresabschluss, Ausführungen **über die Zweckmäßigkeit der eingesetzten Mittel und eine Bewertung dessen**, inwiefern die Agentur **effektiv war und** die vorgegebenen Leistungsindikatoren erfüllt

hat. Der Jahresbericht wird veröffentlicht;

Or. cs

Änderungsantrag 205

Maria Grapini

Vorschlag für eine Verordnung Artikel 14 – Absatz 1 – Buchstabe m

Vorschlag der Kommission

(m) ernennt den Exekutivdirektor und verlängert gegebenenfalls dessen Amtszeit oder enthebt ihn seines Amtes gemäß Artikel 33 dieser Verordnung;

Geänderter Text

(m) ernennt den Exekutivdirektor **durch Auswahlverfahren auf der Grundlage berufsfachlicher Kriterien** und verlängert gegebenenfalls dessen Amtszeit oder enthebt ihn seines Amtes gemäß Artikel 33 dieser Verordnung;

Or. ro

Änderungsantrag 206

Jiří Pospíšil

Vorschlag für eine Verordnung Artikel 14 – Absatz 1 – Buchstabe o

Vorschlag der Kommission

(o) fasst unter Berücksichtigung der Tätigkeitserfordernisse der Agentur und unter Beachtung der Grundsätze einer wirtschaftlichen Haushaltsführung alle Beschlüsse über die Schaffung und, falls notwendig, Änderung der Organisationsstruktur der Agentur;

Geänderter Text

(o) fasst unter Berücksichtigung der **in dieser Verordnung aufgeführten** Tätigkeitserfordernisse der Agentur und unter Beachtung der Grundsätze einer wirtschaftlichen Haushaltsführung alle Beschlüsse über die Schaffung und, falls notwendig, Änderung der Organisationsstruktur der Agentur;

Or. cs

Änderungsantrag 207

Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung

Artikel 18 – Absatz 3

Vorschlag der Kommission

3. Der Exekutivrat besteht aus fünf Mitgliedern, die aus den Reihen der Mitglieder des Verwaltungsrats ernannt werden; darunter befinden sich der Vorsitzende des Verwaltungsrats, der zugleich auch Vorsitzender des Exekutivrats sein kann, und einer der Vertreter der Kommission. Der Exekutivdirektor nimmt an den Sitzungen des Exekutivrats ohne Stimmrecht teil.

Geänderter Text

3. Der Exekutivrat besteht aus fünf Mitgliedern, die aus den Reihen der Mitglieder des Verwaltungsrats **in einem ausgewogenen Verhältnis zwischen Männern und Frauen** ernannt werden; darunter befinden sich der Vorsitzende des Verwaltungsrats, der zugleich auch Vorsitzender des Exekutivrats sein kann, und einer der Vertreter der Kommission. Der Exekutivdirektor nimmt an den Sitzungen des Exekutivrats ohne Stimmrecht teil.

Or. en

Begründung

Es muss eine ausgewogene Vertretung von Frauen und Männern hinzugefügt werden.

Änderungsantrag 208

Evelyne Gebhardt, Kerstin Westphal, Lucy Anderson, Catherine Stihler, Marc Tarabella, Pina Picierno, Christel Schaldemose

Vorschlag für eine Verordnung

Artikel 19 – Absatz 2

Vorschlag der Kommission

2. Der Exekutivdirektor erstattet dem Europäischen Parlament über seine Tätigkeit **Bericht**, wenn er dazu aufgefordert wird. Der Rat kann den Exekutivdirektor auffordern, über seine Tätigkeit Bericht zu erstatten.

Geänderter Text

2. Der Exekutivdirektor erstattet dem Europäischen Parlament über seine Tätigkeit **jährlich, oder** wenn er dazu aufgefordert wird, **Bericht**. Der Rat kann den Exekutivdirektor auffordern, über seine Tätigkeit Bericht zu erstatten.

Or. en

Änderungsantrag 209

Arndt Kohn, Sergio Gutiérrez Prieto, Lucy Anderson, Pina Picierno, Christel Schaldemose

Vorschlag für eine Verordnung
Artikel 20 – Absatz 1

Vorschlag der Kommission

1. Der Verwaltungsrat setzt auf Vorschlag des Exekutivdirektors eine Ständige Gruppe der Interessenträger ein, die sich aus anerkannten Sachverständigen als Vertreter der einschlägigen Interessenträger zusammensetzt, darunter die IKT-Branche, Anbieter öffentlich zugänglicher elektronischer Kommunikationsnetze oder -dienste, Verbrauchergruppen, wissenschaftliche Sachverständige für die Cybersicherheit sowie Vertreter der zuständigen Behörden, die gemäß der [Richtlinie über den Europäischen Kodex für elektronische Kommunikation] notifiziert wurden, sowie Strafverfolgungsbehörden und Datenschutz-Aufsichtsbehörden.

Geänderter Text

1. Der Verwaltungsrat setzt auf Vorschlag des Exekutivdirektors eine Ständige Gruppe der Interessenträger ein, die sich aus anerkannten Sachverständigen als Vertreter der einschlägigen Interessenträger zusammensetzt, darunter die IKT-Branche, Anbieter öffentlich zugänglicher elektronischer Kommunikationsnetze oder -dienste, Verbrauchergruppen, wissenschaftliche Sachverständige für die Cybersicherheit, **das Europäische Forum für Akkreditierungen, Konformitätsbewertungsstellen** sowie Vertreter der zuständigen Behörden, die gemäß der [Richtlinie über den Europäischen Kodex für elektronische Kommunikation] notifiziert wurden, sowie Strafverfolgungsbehörden und Datenschutz-Aufsichtsbehörden.

Or. en

Änderungsantrag 210
Jiří Maštálka

Vorschlag für eine Verordnung
Artikel 20 – Absatz 1

Vorschlag der Kommission

1. Der Verwaltungsrat setzt auf Vorschlag des Exekutivdirektors eine Ständige Gruppe der Interessenträger ein, die sich aus anerkannten Sachverständigen als Vertreter der einschlägigen Interessenträger zusammensetzt, darunter die IKT-Branche, Anbieter öffentlich zugänglicher elektronischer Kommunikationsnetze oder -dienste, Verbrauchergruppen, wissenschaftliche Sachverständige für die Cybersicherheit

Geänderter Text

1. Der Verwaltungsrat setzt auf Vorschlag des Exekutivdirektors eine Ständige Gruppe der Interessenträger ein, die sich aus anerkannten **Sicherheitsexperten** als Vertreter der einschlägigen Interessenträger zusammensetzt, darunter die **europäische** IKT-Branche, **europäische** Anbieter öffentlich zugänglicher elektronischer Kommunikationsnetze oder -dienste, Verbrauchergruppen, wissenschaftliche

sowie Vertreter der zuständigen Behörden, die gemäß der [Richtlinie über den Europäischen Kodex für elektronische Kommunikation] notifiziert wurden, sowie Strafverfolgungsbehörden und Datenschutz-Aufsichtsbehörden.

Sachverständige für die Cybersicherheit sowie Vertreter der zuständigen Behörden, die gemäß der [Richtlinie über den Europäischen Kodex für elektronische Kommunikation] notifiziert wurden, sowie Strafverfolgungsbehörden und Datenschutz-Aufsichtsbehörden.

Or. en

Änderungsantrag 211
Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Artikel 20 – Absatz 1

Vorschlag der Kommission

1. Der Verwaltungsrat setzt auf Vorschlag des Exekutivdirektors eine Ständige Gruppe der Interessenträger ein, die sich aus anerkannten Sicherheitsexperten als Vertreter der einschlägigen Interessenträger zusammensetzt, darunter die IKT-Branche, **Anbieter** öffentlich zugänglicher elektronischer Kommunikationsnetze oder -dienste, Verbrauchergruppen, wissenschaftliche Sachverständige für die Cybersicherheit sowie Vertreter der zuständigen Behörden, die gemäß der [Richtlinie über den Europäischen Kodex für elektronische Kommunikation] notifiziert wurden, sowie Strafverfolgungsbehörden und Datenschutz-Aufsichtsbehörden.

Geänderter Text

1. Der Verwaltungsrat setzt auf Vorschlag des Exekutivdirektors eine Ständige Gruppe der Interessenträger ein, die sich aus anerkannten Sicherheitsexperten als Vertreter der einschlägigen Interessenträger zusammensetzt, darunter die IKT-Branche **in der Union, EU-Anbieter** öffentlich zugänglicher elektronischer Kommunikationsnetze oder -dienste, Verbrauchergruppen, wissenschaftliche Sachverständige für die Cybersicherheit sowie Vertreter der zuständigen Behörden, die gemäß der [Richtlinie über den Europäischen Kodex für elektronische Kommunikation] notifiziert wurden, sowie Strafverfolgungsbehörden und Datenschutz-Aufsichtsbehörden.

Or. en

Änderungsantrag 212
Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung
Artikel 20 – Absatz 2

Vorschlag der Kommission

2. Die Verfahren für die Ständige Gruppe der Interessenträger, die insbesondere die Anzahl, die Zusammensetzung, die Ernennung der Mitglieder durch den Verwaltungsrat, den Vorschlag des Exekutivdirektors und die Arbeitsweise der Gruppe betreffen, werden in den internen Verfahrensvorschriften der Agentur festgelegt und öffentlich bekannt gemacht.

Geänderter Text

2. Die Verfahren für die Ständige Gruppe der Interessenträger, die insbesondere die Anzahl, die Zusammensetzung, die Ernennung der Mitglieder durch den Verwaltungsrat, den Vorschlag des Exekutivdirektors und die Arbeitsweise der Gruppe betreffen, werden in den internen Verfahrensvorschriften der Agentur festgelegt und öffentlich bekannt gemacht. **Die Verfahren entsprechen bewährten Verfahren und stellen eine ausgewogene Vertretung und gleiche Rechte für alle Interessenträger sowie ein ausgewogenes Verhältnis von Frauen und Männern sicher.**

Or. en

Begründung

Um die besten Ergebnisse erzielen zu können, ist eine ausgewogene und faire Vertretung erforderlich.

Änderungsantrag 213

Jan Philipp Albrecht

im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung

Artikel 20 – Absatz 2 a (neu)

Vorschlag der Kommission

Geänderter Text

2a. Zur Ständigen Gruppe der Interessenträger gehören mindestens fünf Verbraucherschutzverbände und zivilgesellschaftliche Organisationen.

Or. en

Begründung

In der aktuellen Ständigen Gruppe der Interessenträger vertritt nur ein Sachverständiger bei dreißig Mitgliedern der Gruppe die Standpunkte der Verbraucher. Das ist nicht ausreichend.

Änderungsantrag 214

Evelyne Gebhardt, Kerstin Westphal, Lucy Anderson, Marc Tarabella

Vorschlag für eine Verordnung

Artikel 20 – Absatz 4

Vorschlag der Kommission

4. Die Amtszeit der Mitglieder der Ständigen Gruppe der Interessenträger beträgt zweieinhalb Jahre. Die Mitglieder des Verwaltungsrats dürfen nicht Mitglieder der Ständigen Gruppe der Interessenträger sein. Sachverständige der Kommission und aus den Mitgliedstaaten können an den Sitzungen der Ständigen Gruppe der Interessenträger teilnehmen und an ihrer Arbeit mitwirken. Vertreter anderer Stellen, die vom Exekutivdirektor für relevant erachtet werden und die der Ständigen Gruppe der Interessenträger nicht angehören, können zur Teilnahme an den Sitzungen der Ständigen Gruppe der Interessenträger und zur Mitarbeit an ihrer Arbeit eingeladen werden.

Geänderter Text

4. Die Amtszeit der Mitglieder der Ständigen Gruppe der Interessenträger beträgt zweieinhalb Jahre. Die Mitglieder des Verwaltungsrats **und des Exekutivrats, mit Ausnahme des in Absatz 3 genannten Exekutivdirektors**, dürfen nicht Mitglieder der Ständigen Gruppe der Interessenträger sein. Sachverständige der Kommission und aus den Mitgliedstaaten können an den Sitzungen der Ständigen Gruppe der Interessenträger teilnehmen und an ihrer Arbeit mitwirken. Vertreter anderer Stellen, die vom Exekutivdirektor für relevant erachtet werden und die der Ständigen Gruppe der Interessenträger nicht angehören, können zur Teilnahme an den Sitzungen der Ständigen Gruppe der Interessenträger und zur Mitarbeit an ihrer Arbeit eingeladen werden.

Or. en

Änderungsantrag 215

Anneleen Van Bossuyt, Daniel Dalton

Vorschlag für eine Verordnung

Artikel 20 – Absatz 5

Vorschlag der Kommission

5. Die Ständige Gruppe der Interessenträger berät die Agentur bei der Durchführung ihrer Tätigkeiten. Sie berät insbesondere den Exekutivdirektor bei der Ausarbeitung eines Vorschlags für das Arbeitsprogramm der Agentur und bei der Gewährleistung der Kommunikation mit

Geänderter Text

5. Die Ständige Gruppe der Interessenträger berät die Agentur bei der Durchführung ihrer Tätigkeiten. Sie berät insbesondere den Exekutivdirektor bei der Ausarbeitung eines Vorschlags für das Arbeitsprogramm der Agentur und bei der Gewährleistung der Kommunikation mit

den einschlägigen Interessenträgern bezüglich aller Fragen im Zusammenhang mit dem Arbeitsprogramm.

den einschlägigen Interessenträgern bezüglich aller Fragen im Zusammenhang mit dem Arbeitsprogramm. ***Ebenso kann sie auf Eigeninitiative oder nach Vorlage von Vorschlägen einschlägiger Interessenträger vorschlagen, dass die Kommission die Agentur auffordert, mögliche europäische Systeme für die Cybersicherheitszertifizierung nach Artikel 44 auszuarbeiten.***

Or. en

Änderungsantrag 216 **Jiří Maštálka**

Vorschlag für eine Verordnung **Artikel 20 – Absatz 5**

Vorschlag der Kommission

5. Die Ständige Gruppe der Interessenträger berät die Agentur bei der Durchführung ihrer Tätigkeiten. Sie berät insbesondere den Exekutivdirektor bei der Ausarbeitung eines Vorschlags für das Arbeitsprogramm der Agentur und bei der Gewährleistung der Kommunikation mit den einschlägigen Interessenträgern bezüglich aller Fragen im Zusammenhang mit dem Arbeitsprogramm.

Geänderter Text

5. Die Ständige Gruppe der Interessenträger berät die Agentur bei der Durchführung ihrer Tätigkeiten. Sie berät insbesondere den Exekutivdirektor bei der Ausarbeitung eines Vorschlags für das Arbeitsprogramm der Agentur und bei der Gewährleistung der Kommunikation mit den einschlägigen Interessenträgern bezüglich aller Fragen im Zusammenhang mit dem Arbeitsprogramm. ***Sie gibt die förmliche Genehmigung für von der Agentur ausgearbeitete mögliche Zertifizierungssysteme, bevor sie der Europäischen Kommission zur Billigung übermittelt werden.***

Or. en

Begründung

Obligatorische Validierung aller möglichen Zertifizierungssysteme durch die Ständige Gruppe der Interessenträger der ENISA, in der Cybersicherheitsexperten zusammenkommen, die vom Cybersicherheitsökosystem und der Wissenschaft als solche anerkannt sind und somit für eine gerechte und offene Steuerung sorgen.

Änderungsantrag 217
Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Artikel 20 – Absatz 5 a (neu)

Vorschlag der Kommission

Geänderter Text

5a. Die Ständige Gruppe der Interessenträger tritt mindestens viermal im Jahr zusammen. Die Tagesordnung mindestens eines dieser Treffen befasst sich mit den in den Artikeln 43 bis 54 [Titel III] genannten Angelegenheiten.

Or. en

Änderungsantrag 218
Nicola Danti, Maria Grapini, Sergio Gutiérrez Prieto, Lucy Anderson, Arndt Kohn, Pina Picierno, Marc Tarabella

Vorschlag für eine Verordnung
Artikel 20 – Absatz 5 a (neu)

Vorschlag der Kommission

Geänderter Text

5a. Sie berät die Agentur, wenn diese mögliche Systeme ausarbeitet.

Or. en

Änderungsantrag 219
Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung
Artikel 23 – Absatz 2

Vorschlag der Kommission

Geänderter Text

2. Die Agentur stellt sicher, dass die Öffentlichkeit sowie interessierte Kreise angemessene, objektive, zuverlässige und leicht zugängliche Informationen, insbesondere zu ihren eigenen

2. Die Agentur stellt sicher, dass die Öffentlichkeit sowie interessierte Kreise angemessene, objektive, zuverlässige und leicht zugängliche Informationen, insbesondere zu **den Debatten und** ihren

Arbeitsergebnissen, erhalten. Ferner veröffentlicht sie die nach Artikel 22 abgegebenen Interessenerklärungen.

eigenen Arbeitsergebnissen, erhalten. Ferner veröffentlicht sie die nach Artikel 22 abgegebenen Interessenerklärungen.

Or. en

Begründung

Transparenz muss unter Berücksichtigung von Art. 24 rechtskräftig sein.

Änderungsantrag 220

Jan Philipp Albrecht

im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung

Artikel 34 – Absatz 2

Vorschlag der Kommission

2. Der Verwaltungsrat beschließt eine Regelung über zur Agentur abgeordnete nationale Sachverständige.

Geänderter Text

2. Der Verwaltungsrat beschließt eine Regelung über zur Agentur abgeordnete nationale Sachverständige, ***in der unter anderem kostenlose Verfahren untersagt und eine gerechte Vergütung gefördert werden.***

Or. en

Begründung

Gleiche Bezahlung für gleiche Arbeit: Um das beste Personal zu bekommen, ist es unakzeptabel, dass die EU Sachverständige aus unterschiedlichen Mitgliedstaaten mit unterschiedlichen nationalen Gehältern mit denselben Aufgaben betraut.

Änderungsantrag 221

Jan Philipp Albrecht

im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung

Artikel 41 – Absatz 2

Vorschlag der Kommission

2. Der Sitzmitgliedstaat der Agentur gewährleistet die bestmöglichen

Geänderter Text

2. Der Sitzmitgliedstaat der Agentur gewährleistet die bestmöglichen

Voraussetzungen für das reibungslose Funktionieren der Agentur, einschließlich der Erreichbarkeit des Standortes, des Vorhandenseins adäquater Bildungseinrichtungen für die Kinder der Mitglieder des Personals und eines angemessenen Zugangs zu Arbeitsmarkt, Sozialversicherung und medizinischer Versorgung für Kinder und Ehegatten.

Voraussetzungen für das reibungslose Funktionieren der Agentur, einschließlich der Erreichbarkeit des Standortes **des Sitzes und anderer Niederlassungen von internationalen Flughäfen aus**, des Vorhandenseins adäquater Bildungseinrichtungen für die Kinder der Mitglieder des Personals und eines angemessenen Zugangs zu Arbeitsmarkt, Sozialversicherung und medizinischer Versorgung für Kinder und Ehegatten.

Or. en

Begründung

Während der Sitzmitgliedstaat außerhalb des Anwendungsbereichs dieser Verordnung liegt, liegt die Sicherstellung der besten Bedingungen für die reibungslose Arbeit der Agentur innerhalb des Geltungsbereichs und dafür werden hier Leitlinien gegeben.

Änderungsantrag 222

Philippe Juvin, Andreas Schwab

Vorschlag für eine Verordnung

Artikel 43 – Absatz 1

Vorschlag der Kommission

Ein europäisches System für die Cybersicherheitszertifizierung dient der Bescheinigung, dass die nach einem solchen System zertifizierten IKT-Produkte und -Dienste auf einer bestimmten Vertrauenswürdigkeitsstufe den festgelegten Anforderungen an ihre Fähigkeit genügen, Handlungen zu widerstehen, die darauf abzielen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übermittelten oder verarbeiteten Daten, Funktionen oder Diensten zu beeinträchtigen, die von diesen Produkten, Prozessen, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden.

Geänderter Text

Ein europäisches System für die Cybersicherheitszertifizierung **wird eingeführt, um das Sicherheitsniveau auf dem digitalen Binnenmarkt zu erhöhen, einen harmonisierten EU-weiten Ansatz für die europäische Zertifizierung zu verfolgen und so sicherzustellen, dass IKT-Produkte, -Dienste und -Systeme gegen Cyberangriffe gewappnet sind.** Es dient der Bescheinigung, dass die nach einem solchen System zertifizierten IKT-Produkte und -Dienste auf einer bestimmten Vertrauenswürdigkeitsstufe den festgelegten **gemeinsamen** Anforderungen an ihre Fähigkeit genügen, Handlungen zu widerstehen, die darauf abzielen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übermittelten oder

verarbeiteten Daten, Funktionen oder Diensten zu beeinträchtigen, die von diesen Produkten, Prozessen, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden.

Or. fr

Änderungsantrag 223
Jiří Maštálka

Vorschlag für eine Verordnung
Artikel 43 – Absatz 1

Vorschlag der Kommission

Ein europäisches System für die Cybersicherheitszertifizierung dient der Bescheinigung, dass die nach einem solchen System zertifizierten IKT-Produkte und -Dienste **auf einer bestimmten Vertrauenswürdigkeitsstufe** den festgelegten Anforderungen an ihre Fähigkeit genügen, **Handlungen zu widerstehen, die darauf abzielen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übermittelten oder verarbeiteten Daten, Funktionen oder Diensten zu beeinträchtigen, die von diesen Produkten, Prozessen, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden.**

Geänderter Text

Ein europäisches System für die Cybersicherheitszertifizierung dient der Bescheinigung, dass die nach einem solchen System zertifizierten IKT-Produkte, **-Prozesse** und -Dienste den **gemäß den Normen** festgelegten Anforderungen an ihre Fähigkeit genügen, **bestimmte Sicherheitsziele zu erfüllen.**

Or. en

Begründung

Das europäische System für die Cybersicherheitszertifizierung sollte einen flexiblen Ansatz je nach den Risikograden und Verwendungen eines Produkts, Dienstes oder Prozesses verfolgen.

Änderungsantrag 224
Roberta Metsola, Eva Maydell, Lara Comi, Carlos Coelho

Vorschlag für eine Verordnung
Artikel 43 – Absatz 1

Vorschlag der Kommission

Ein europäisches System für die Cybersicherheitszertifizierung dient der Bescheinigung, dass die nach einem solchen System zertifizierten **IKT-Produkte** und -Dienste auf einer bestimmten Vertrauenswürdigkeitsstufe den festgelegten Anforderungen an ihre Fähigkeit genügen, Handlungen zu widerstehen, die darauf abzielen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übermittelten oder verarbeiteten Daten, Funktionen oder Diensten zu beeinträchtigen, die von diesen **Produkten, Prozessen**, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden.

Geänderter Text

Ein europäisches System für die Cybersicherheitszertifizierung dient der Bescheinigung, dass die nach einem solchen System zertifizierten **IKT-Hardware- und Software-Produkte** und -Dienste auf einer bestimmten **risikobasierten** Vertrauenswürdigkeitsstufe den festgelegten Anforderungen an ihre Fähigkeit genügen, Handlungen zu widerstehen, die darauf abzielen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übermittelten oder verarbeiteten Daten, Funktionen oder Diensten zu beeinträchtigen, die von diesen **Hardware- und Software-Produkten, Entwicklungs- und Instandhaltungsprozessen**, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden.

Or. en

Änderungsantrag 225
Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Artikel 43 – Absatz 1

Vorschlag der Kommission

Ein europäisches System für die Cybersicherheitszertifizierung dient der Bescheinigung, dass die nach einem solchen System zertifizierten IKT-Produkte **und** -Dienste auf einer bestimmten Vertrauenswürdigkeitsstufe den festgelegten Anforderungen **an ihre** Fähigkeit genügen, Handlungen zu widerstehen, die darauf abzielen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übermittelten oder verarbeiteten Daten,

Geänderter Text

Ein europäisches System für die Cybersicherheitszertifizierung dient der Bescheinigung, dass die nach einem solchen System zertifizierten IKT-Produkte, -Dienste **und -Prozesse** auf einer bestimmten Vertrauenswürdigkeitsstufe den festgelegten Anforderungen **und Eigenschaften hinsichtlich ihrer** Fähigkeit genügen, Handlungen zu widerstehen, die darauf abzielen, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten,

Funktionen oder Diensten zu beeinträchtigen, die von diesen Produkten, Prozessen, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden.

übermittelten oder verarbeiteten Daten, Funktionen oder Diensten zu beeinträchtigen, die von diesen Produkten, Prozessen, Diensten und Systemen angeboten oder über diese zugänglich gemacht werden.

Or. en

Änderungsantrag 226
Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung
Artikel 43 a (neu)

Vorschlag der Kommission

Geänderter Text

Artikel 43a

Sicherheit durch Technikgestaltung und durch Voreinstellungen

1. Die Hersteller und Dienstleister sorgen bei ihren IKT-Produkten und -Diensten unter Berücksichtigung des Stands der Technik für standardmäßig eingebaute Sicherheit. Die Hersteller und Dienstleister müssen sicherstellen, dass die Software auf ihren IKT-Produkten oder bei ihren IKT-Diensten sicher ist, und unter Berücksichtigung des aktuellen Stands der Technik keine Sicherheitslücke bekannt ist. IKT-Produkte und -Dienste müssen folgende technischen Maßnahmen erfüllen:

(a) IKT-Produkte und -Dienste müssen mit aktueller Software ausgestattet werden und Mechanismen für den Empfang regelmäßiger, ordnungsgemäß authentifizierter und aus vertrauenswürdiger Quelle stammender Aktualisierungen enthalten;

(b) Fernzugriffsmöglichkeiten auf das IKT-Produkt bzw. den IKT-Dienst müssen dokumentiert und spätestens bei der Installation gegen den unbefugten Zugriff

gesichert werden;

(c) IKT-Produkte dürfen nicht dieselben fest kodierte Standardkennwörter für alle Geräte haben;

(d) Durch IKT-Produkte und -Dienste gespeicherte Daten müssen durch modernste Methoden wie Verschlüsselung geschützt werden;

(e) IKT-Produkte und -Dienste dürfen für die Authentifizierung nur Hochsicherheitsmethoden zulassen.

2. Die Hersteller und Dienstleister müssen die zuständige Behörde über alle bekannten Sicherheitsschwachstellen informieren, sobald sie entdeckt werden. Außerdem müssen sie für eine zeitnahe Reparatur und/oder einen zeitnahen Austausch sorgen, um alle neu entdeckten Sicherheitslücken zu beheben.

3. In den Verkehr gebrachte IKT-Produkte und -Dienste müssen für die vorhersehbare und normale Nutzungsdauer die in Absatz 1 aufgeführten Anforderungen erfüllen.

4. Die Kommission erlässt über Durchführungsakte und in Absprache mit der ENISA spezielle Regeln zu den Spezifitäten der in Absatz 1 angeführten Sicherheitsanforderungen.

5. Haben die Marktüberwachungsbehörden Anlass zu der Annahme, dass das IKT-Produkt oder der IKT-Dienst die Anforderungen dieser Verordnung nicht erfüllt, so schreiben sie dem betroffenen Hersteller bzw. Dienstleister unverzüglich vor, innerhalb einer der Art des Risikos angemessenen Frist entweder alle geeigneten Korrekturmaßnahmen zu treffen, um die Übereinstimmung des Produkts mit diesen Anforderungen herzustellen, es vom Markt zu nehmen oder es zurückzurufen.

6. Ergreift der Hersteller oder Dienstleister innerhalb der in Absatz 5

genannten Frist keine angemessenen Abhilfemaßnahmen, so treffen die Marktüberwachungsbehörden alle geeigneten vorläufigen Maßnahmen, um die Bereitstellung des Produkts auf ihrem nationalen Markt zu untersagen oder einzuschränken, das Produkt vom Markt zu nehmen oder zurückzurufen.

7. Die Marktüberwachungsbehörden organisieren angemessene Kontrollen der Produktkonformität und verpflichten die Hersteller bzw. die Dienstleister, nichtkonforme Produkte vom Markt zu nehmen. Bei der Ermittlung der Produkte, die einer Konformitätskontrolle unterzogen werden sollen, geben die nationalen Zertifizierungsbehörden für Verbraucher bestimmten Hochrisikoprodukten, in neue Technologien eingebetteten Produkten und/oder Produkten mit hohen Verkaufsraten den Vorrang.

Or. en

Begründung

One of the key reasons behind the increase of cyberattacks is the lack of security functionalities incorporated in the design of the connected products and/or services. Today, most of the connected devices available in the EU's single market are designed and manufactured without the most basic security features embedded in their software. In order to trust the Internet of Things, consumers must be assured that the connected products they purchase or services they use are secure and protected from software and hardware vulnerabilities. To ensure a high-level of security by design and by default, a minimum set of requirements for security should be binding for all connected products as a condition for putting them on the market. Such a horizontal and binding framework should be established as a complement of existing and pending legislation that requires cybersecurity measures such as the General Data Protection Regulation and the proposal for a European Electronic Communication Code.

Änderungsantrag 227
Jiří Maštálka

Vorschlag für eine Verordnung
Artikel 43 a (neu)

Vorschlag der Kommission

Geänderter Text

Artikel 43a

Arbeitsplan

Die Kommission richtet in Absprache mit dem in Artikel 44 genannten beratenden Ausschuss spätestens sechs Monate nach dem Inkrafttreten der Verordnung und danach alle zwei Jahre einen Arbeitsplan ein, der öffentlich zugänglich gemacht wird.

Or. en

Begründung

Die Veröffentlichung des Arbeitsplans würde die Transparenz und Rechenschaftspflicht der Entwicklung von Zertifizierungssystemen auf EU-Ebene verbessern.

Änderungsantrag 228

Mylène Troszczynski

Vorschlag für eine Verordnung

Artikel 44 – Absatz 1

Vorschlag der Kommission

Geänderter Text

1. ***Im Auftrag der Kommission arbeitet die ENISA ein mögliches europäisches System für die Cybersicherheitszertifizierung aus, das den in den Artikeln 45, 46 und 47 genannten Anforderungen genügt.*** Die Mitgliedstaaten oder die ***nach Artikel 53 eingesetzte*** Europäische Gruppe für die Cybersicherheitszertifizierung (im Folgenden die „Gruppe“) ***kann der Kommission die Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung vorschlagen.***

1. Die Mitgliedstaaten oder die Europäische Gruppe für die Cybersicherheitszertifizierung (im Folgenden die „Gruppe“) ***arbeiten bzw. arbeitet ein europäisches System für die Cybersicherheitszertifizierung aus, das den Anforderungen genügt, die von den Mitgliedstaaten in den Artikeln 45, 46 und 47 der vorliegenden Verordnung festgelegt wurden.***

Or. fr

Änderungsantrag 229
Anneleen Van Bossuyt, Daniel Dalton

Vorschlag für eine Verordnung
Artikel 44 – Absatz 1

Vorschlag der Kommission

1. Im Auftrag der Kommission arbeitet die ENISA ein mögliches europäisches System für die Cybersicherheitszertifizierung aus, das den in den Artikeln 45, 46 und 47 genannten Anforderungen genügt. Die Mitgliedstaaten *oder* die nach Artikel 53 eingesetzte Europäische Gruppe für die Cybersicherheitszertifizierung (im Folgenden die „Gruppe“) *kann* der Kommission die Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung vorschlagen.

Geänderter Text

1. Im Auftrag der Kommission arbeitet die ENISA ein mögliches europäisches System für die Cybersicherheitszertifizierung aus, das den in den Artikeln 45, 46 und 47 genannten Anforderungen genügt. Die Mitgliedstaaten, *die Ständige Gruppe der Interessenträger, entweder auf Eigeninitiative oder nach Vorlage von Vorschlägen durch die Interessenträger und* die nach Artikel 53 eingesetzte Europäische Gruppe für die Cybersicherheitszertifizierung (im Folgenden die „Gruppe“) *können* der Kommission die Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung vorschlagen.

Or. en

Änderungsantrag 230
Dita Charanzová

Vorschlag für eine Verordnung
Artikel 44 – Absatz 1

Vorschlag der Kommission

1. Im Auftrag der Kommission arbeitet die ENISA ein mögliches europäisches System für die Cybersicherheitszertifizierung aus, das den in den Artikeln 45, 46 und 47 genannten Anforderungen genügt. *Die Mitgliedstaaten oder die nach Artikel 53 eingesetzte Europäische Gruppe für die Cybersicherheitszertifizierung (im Folgenden die „Gruppe“) kann der Kommission die Ausarbeitung eines*

Geänderter Text

1. *Die Mitgliedstaaten, die nach Artikel 20 eingesetzte Ständige Gruppe der Interessenträger oder Branchenvertreter können der Kommission oder der Europäischen Gruppe für die Cybersicherheitszertifizierung (im Folgenden die „Gruppe“) die Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung*

möglichen europäischen Systems für die Cybersicherheitszertifizierung vorschlagen.

vorschlagen. Im Auftrag der Kommission **oder der Gruppe** arbeitet die ENISA ein mögliches europäisches System für die Cybersicherheitszertifizierung aus, das den in den Artikeln 45, 46 und 47 genannten Anforderungen genügt.

Or. en

Änderungsantrag 231

Jan Philipp Albrecht

im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung Artikel 44 – Absatz 1

Vorschlag der Kommission

1. Im Auftrag der Kommission arbeitet die ENISA ein mögliches europäisches System für die **Cybersicherheitszertifizierung** aus, das den in den Artikeln 45, 46 und 47 genannten Anforderungen genügt. Die Mitgliedstaaten **oder** die nach Artikel 53 eingesetzte Europäische Gruppe für die Cybersicherheitszertifizierung (im Folgenden die „Gruppe“) kann der Kommission die Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung vorschlagen.

Geänderter Text

1. Im Auftrag der Kommission arbeitet die ENISA ein mögliches europäisches System für die **IT-Sicherheitszertifizierung** aus, das den in den Artikeln 45, 46 und 47 genannten Anforderungen genügt. Die Mitgliedstaaten, die nach Artikel 53 eingesetzte Europäische Gruppe für die Cybersicherheitszertifizierung (im Folgenden die „Gruppe“) **oder die nach Artikel 20 eingesetzte Ständige Gruppe der Interessenträger** kann der Kommission die Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung vorschlagen.

Or. en

Begründung

Es ist von entscheidender Bedeutung, dass alle Sachverständigen während der Ausarbeitung eines Zertifizierungssystems innerhalb der ENISA systematisch und regelmäßig konsultiert werden.

Änderungsantrag 232

Jiří Maštálka

**Vorschlag für eine Verordnung
Artikel 44 – Absatz 1 a (neu)**

Vorschlag der Kommission

Geänderter Text

1a. Die ENISA setzt mit Unterstützung der Europäischen Kommission und der Mitgliedstaaten einen beratenden Ausschuss ein, an dem die Europäische Gruppe für die Cybersicherheitszertifizierung und alle interessierten Kreise, wie die Industrie, einschließlich KMU, Gewerkschaften, Normungsorganisationen, Händler, Einzelhändler, Importeure oder Endverbraucher, die mit dem betreffenden IKT-Produkt, -Prozess oder -Dienst zu tun haben, ausgewogen beteiligt werden.

Dieser Ausschuss wird in jede Phase der Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung einbezogen, einschließlich der Festlegung seiner Elemente und Sicherheitsanforderungen. Der beratende Ausschuss wird mindestens vor der Ausarbeitung eines möglichen Systems, mindestens einmal, wenn der erste Entwurf eines möglichen Systems zur Verfügung steht, sowie vor der Annahme der Durchführungsbestimmungen zu Rate gezogen. Der beratende Ausschuss kann bei der ENISA einen Antrag auf die Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung stellen, auch um Initiativen aus der Branche aufzunehmen.

Or. en

Änderungsantrag 233

Catherine Stihler, Liisa Jaakonsaari, Christel Schaldemose

Vorschlag für eine Verordnung

Artikel 44 – Absatz 2

Vorschlag der Kommission

2. Bei der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert die ENISA alle in Frage kommenden Interessenträger und arbeitet eng mit der Gruppe zusammen. Die Gruppe leistet die von der ENISA für die Ausarbeitung des möglichen Systems geforderte Unterstützung und fachliche Beratung und gibt nötigenfalls auch eine Stellungnahme hierzu ab.

Geänderter Text

2. Bei der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert die ENISA alle in Frage kommenden Interessenträger und arbeitet eng mit der Gruppe zusammen. Die Gruppe leistet die von der ENISA für die Ausarbeitung des möglichen Systems geforderte Unterstützung und fachliche Beratung und gibt nötigenfalls auch eine Stellungnahme hierzu ab. ***Die ENISA stellt die Beteiligung von Vertretern der Mitgliedstaaten und aller wichtigen Parteien sicher, die von der betreffenden IKT-Produktgruppe oder dem betreffenden IKT-Dienst betroffen sind. Dazu gehören Parteien entlang der Wertschöpfungskette wie Gewerkschaften, Händler, Einzelhändler, Importeure, Konformitätsbewertungsstellen, Endkunden und andere. Ebenso werden Wirtschaftsakteure wie unter anderem Hersteller, Anbieter von Cybersicherheitslösungen, Systemintegratoren, Sicherheitsexperten und Anlagenbesitzer einbezogen.***

Or. en

Änderungsantrag 234

Anneleen Van Bossuyt, Daniel Dalton

Vorschlag für eine Verordnung

Artikel 44 – Absatz 2

Vorschlag der Kommission

2. ***Bei*** der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert die ENISA alle in Frage kommenden Interessenträger und arbeitet eng mit der Gruppe zusammen. ***Die*** Gruppe ***leistet*** die von der ENISA für die Ausarbeitung des möglichen Systems

Geänderter Text

2. ***Während*** der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert die ENISA alle in Frage kommenden Interessenträger und arbeitet eng mit der Gruppe zusammen. ***Die jeweiligen Interessenträger und die*** Gruppe ***leisten*** die von der ENISA für die

geforderte Unterstützung und fachliche Beratung und **gibt** nötigenfalls auch eine Stellungnahme hierzu ab.

Ausarbeitung des möglichen Systems geforderte Unterstützung und fachliche Beratung und **geben** nötigenfalls auch eine Stellungnahme hierzu ab. **Gegebenenfalls kann die ENISA auch eine Sachverständigengruppe an Interessenträgern einrichten, bestehend aus Mitgliedern der Ständigen Gruppe der Interessenträger und anderen in Frage kommenden Interessenträgern mit spezifischem Fachwissen auf dem Gebiet eines bestimmten möglichen Systems, um weitere Unterstützung und Beratung bereitzustellen.**

Or. en

Änderungsantrag 235
Roberta Metsola, Lara Comi, Carlos Coelho

Vorschlag für eine Verordnung
Artikel 44 – Absatz 2

Vorschlag der Kommission

2. Bei der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert die ENISA alle in Frage kommenden Interessenträger und arbeitet eng mit der Gruppe zusammen. Die Gruppe leistet die von der ENISA für die Ausarbeitung des möglichen Systems geforderte Unterstützung und fachliche Beratung und gibt nötigenfalls auch eine Stellungnahme hierzu ab.

Geänderter Text

2. Bei der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert die ENISA alle in Frage kommenden Interessenträger und arbeitet eng mit der Gruppe zusammen, **um die Sicherheitsziele des möglichen Zertifizierungssystems im Einklang mit Artikel 45 festzulegen und darauf aufbauend eine Checkliste für die Risiken und die entsprechenden Cybersicherheitsmerkmale zu erstellen.** Die Gruppe leistet die von der ENISA für die Ausarbeitung des möglichen Systems geforderte Unterstützung und fachliche Beratung und gibt nötigenfalls auch eine Stellungnahme hierzu ab.

Or. en

Änderungsantrag 236

Dita Charanzová, Morten Løkkegaard

**Vorschlag für eine Verordnung
Artikel 44 – Absatz 2**

Vorschlag der Kommission

2. Bei der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert die ENISA **alle** in Frage kommenden Interessenträger und arbeitet eng mit der Gruppe zusammen. Die Gruppe **leistet die von der ENISA für die Ausarbeitung des möglichen Systems geforderte Unterstützung und fachliche Beratung und gibt nötigenfalls auch eine Stellungnahme hierzu ab.**

Geänderter Text

2. Bei der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert die ENISA **die Ständige Gruppe der Interessenträger, insbesondere die europäischen Normungsgremien, und alle anderen** in Frage kommenden Interessenträger **in einem formalen, standardisierten und transparenten Verfahren** und arbeitet eng mit der Gruppe zusammen. Die Gruppe **und alle anderen in Frage kommenden Interessenträger unterstützen die ENISA bei der Ausarbeitung des möglichen Systems und bieten ihr diesbezüglich fachliche Beratung, unter anderem durch die Abgabe von Stellungnahmen.**

Or. en

**Änderungsantrag 237
Antanas Guoga**

**Vorschlag für eine Verordnung
Artikel 44 – Absatz 2**

Vorschlag der Kommission

2. Bei der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert die ENISA alle in Frage kommenden Interessenträger und arbeitet eng mit der Gruppe zusammen. Die Gruppe **leistet die von der ENISA für die Ausarbeitung des möglichen Systems geforderte Unterstützung und fachliche Beratung und gibt** nötigenfalls auch eine Stellungnahme hierzu ab.

Geänderter Text

2. Bei der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert die ENISA alle in Frage kommenden Interessenträger **in einem formalen, standardisierten und transparenten Verfahren** und arbeitet eng mit der Gruppe zusammen. Die Gruppe **und alle in Frage kommenden Interessenträger leisten die von der ENISA für die Ausarbeitung des möglichen Systems geforderte Unterstützung und fachliche Beratung und geben** nötigenfalls auch eine

Stellungnahme hierzu ab.

Or. en

Änderungsantrag 238
Jan Philipp Albrecht
im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung
Artikel 44 – Absatz 2

Vorschlag der Kommission

2. Bei der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert die ENISA alle in Frage kommenden Interessenträger und arbeitet eng mit der Gruppe zusammen. Die Gruppe leistet die von der ENISA für die Ausarbeitung des möglichen Systems geforderte Unterstützung und fachliche Beratung und gibt nötigenfalls auch eine Stellungnahme hierzu ab.

Geänderter Text

2. Bei der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert die ENISA alle in Frage kommenden Interessenträger und arbeitet eng mit der Gruppe **sowie mit den Verbraucherschutzverbänden, der Artikel-29-Datenschutzgruppe und dem Europäischen Datenschutzausschuss** zusammen. Die Gruppe leistet die von der ENISA für die Ausarbeitung des möglichen Systems geforderte Unterstützung und fachliche Beratung und gibt nötigenfalls auch eine Stellungnahme hierzu ab.

Or. en

Begründung

Dies geht auf die Stellungnahme des EDSB zurück. Die Erzeugung von Synergieeffekten ist mit Blick auf die Technologie und eine verantwortungsvolle Verwaltung äußerst wichtig, damit die Organisationen, die sich bemühen, den einschlägigen Instrumenten Rechnung zu tragen, nicht den Eindruck erhalten, dass die im Zusammenhang mit dem europäischen Rahmen für die Cybersicherheitszertifizierung und der Datenschutz-Grundverordnung erteilten Zertifizierungen widersprüchlich oder irrelevant sind.

Änderungsantrag 239
Lucy Anderson, Sergio Gutiérrez Prieto, Kerstin Westphal, Marc Tarabella, Christel Schaldemose, Liisa Jaakonsaari

Vorschlag für eine Verordnung
Artikel 44 – Absatz 2

Vorschlag der Kommission

2. Bei der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert die ENISA alle in Frage kommenden Interessenträger und arbeitet eng mit der Gruppe zusammen. Die Gruppe leistet die von der ENISA für die Ausarbeitung des möglichen Systems geforderte Unterstützung und fachliche Beratung und gibt nötigenfalls auch eine Stellungnahme hierzu ab.

Änderungsantrag

2. Bei der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert die ENISA alle in Frage kommenden Interessenträger, **darunter einschlägige Vertreter der Zivilgesellschaft wie Verbraucherschutzverbände**, und arbeitet eng mit der Gruppe zusammen. Die Gruppe leistet die von der ENISA für die Ausarbeitung des möglichen Systems geforderte Unterstützung und fachliche Beratung und gibt nötigenfalls auch eine Stellungnahme hierzu ab.

Or. en

Änderungsantrag 240
Andreas Schwab, Philippe Juvin

Vorschlag für eine Verordnung
Artikel 44 – Absatz 2

Vorschlag der Kommission

2. Bei der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert **die ENISA** alle in Frage kommenden Interessenträger und arbeitet eng mit der Gruppe zusammen. Die Gruppe leistet die von der ENISA für die Ausarbeitung des möglichen Systems geforderte Unterstützung und fachliche Beratung und gibt nötigenfalls auch eine Stellungnahme hierzu ab.

Geänderter Text

2. Bei der Ausarbeitung der möglichen Systeme nach Absatz 1 **berücksichtigt die ENISA bereits bestehende nationale und internationale Normen. Die ENISA** konsultiert alle in Frage kommenden Interessenträger und arbeitet eng mit der Gruppe zusammen. Die Gruppe leistet die von der ENISA für die Ausarbeitung des möglichen Systems geforderte Unterstützung und fachliche Beratung und gibt nötigenfalls auch eine Stellungnahme hierzu ab.

Or. en

Änderungsantrag 241
Jiří Maštálka

Vorschlag für eine Verordnung
Artikel 44 – Absatz 2

Vorschlag der Kommission

2. Bei der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert die ENISA alle in Frage kommenden Interessenträger und arbeitet eng mit der Gruppe zusammen. Die Gruppe leistet die von der ENISA für die Ausarbeitung des möglichen Systems geforderte Unterstützung und fachliche Beratung und gibt nötigenfalls auch eine Stellungnahme hierzu ab.

Geänderter Text

2. Bei der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert die ENISA **den beratenden Ausschuss und** alle in Frage kommenden Interessenträger und arbeitet eng mit der Gruppe zusammen. Die Gruppe leistet die von der ENISA für die Ausarbeitung des möglichen Systems geforderte Unterstützung und fachliche Beratung und gibt nötigenfalls auch eine Stellungnahme hierzu ab.

Or. en

Änderungsantrag 242
Mylène Troszczyński

Vorschlag für eine Verordnung
Artikel 44 – Absatz 2

Vorschlag der Kommission

2. Bei der Ausarbeitung der möglichen Systeme **nach Absatz 1** konsultiert die ENISA alle in Frage kommenden Interessenträger und arbeitet eng mit der Gruppe zusammen. Die Gruppe leistet die von der ENISA für die Ausarbeitung des möglichen Systems geforderte Unterstützung und fachliche Beratung und gibt nötigenfalls auch eine Stellungnahme hierzu ab.

Geänderter Text

2. Bei der Ausarbeitung der möglichen Systeme konsultiert die ENISA alle in Frage kommenden Interessenträger und arbeitet eng mit der Gruppe zusammen. Die Gruppe leistet die von der ENISA für die Ausarbeitung des möglichen Systems geforderte Unterstützung und fachliche Beratung und gibt nötigenfalls auch eine Stellungnahme hierzu ab.

Or. fr

Änderungsantrag 243
Roberta Metsola, Lara Comi, Pascal Arimont, Andreas Schwab, Carlos Coelho

Vorschlag für eine Verordnung
Artikel 44 – Absatz 2 a (neu)

Vorschlag der Kommission

Geänderter Text

2a. Die ENISA koordiniert die Zusammenstellung einer Checkliste der Risiken in Verbindung mit der Hardware oder Software des IKT-Produkts oder -Dienstes. Die Risiken werden den entsprechenden Cybersicherheitsmerkmalen zugeordnet, die in das mögliche europäische System für die Cybersicherheitszertifizierung eingefügt werden.

Or. en

Änderungsantrag 244
Mylène Troszczynski

Vorschlag für eine Verordnung
Artikel 44 – Absatz 2 a (neu)

Vorschlag der Kommission

Geänderter Text

2a. Der Zertifizierungsrahmen sollte von dem Fachwissen der Mitgliedstaaten profitieren, die in diesen strategischen Fragen langjährige Erfahrung haben, und von Branchen unterstützt werden, die über umfangreiches Wissen in diesem Bereich verfügen.

Or. fr

Änderungsantrag 245
Catherine Stihler, Liisa Jaakonsaari

Vorschlag für eine Verordnung
Artikel 44 – Absatz 2 a (neu)

Vorschlag der Kommission

Geänderter Text

2a. Die ENISA versucht, alle nach Absatz 1 dieses Artikels ausgearbeiteten möglichen europäischen Systeme für die

Cybersicherheitszertifizierung im größtmöglichen Maße auf die entsprechenden international anerkannten Normen abzustimmen.

Or. en

Änderungsantrag 246
Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Artikel 44 – Absatz 2 a (neu)

Vorschlag der Kommission

Geänderter Text

2a. Alle bei der Erfüllung ihrer Aufgaben im Rahmen dieser Verordnung erhaltenen Informationen fallen unter die Geheimhaltungspflicht der ENISA.

Or. en

Änderungsantrag 247
Roberta Metsola, Lara Comi, Pascal Arimont, Andreas Schwab, Carlos Coelho

Vorschlag für eine Verordnung
Artikel 44 – Absatz 2 b (neu)

Vorschlag der Kommission

Geänderter Text

2b. Die ausgearbeitete Checkliste stützt sich auf die Erfahrung der Mitgliedstaaten im Zusammenhang mit der Konzeption und der Umsetzung von Cybersicherheitszertifikaten in ihrem Hoheitsgebiet. Es wird eine Liste erwarteter Risiken aufgestellt, die sich auf eine Bewertung des Risikoumfelds, in dem das IKT-Software- oder Hardwareprodukt bzw. der IKT-Dienst letztendlich eingesetzt wird, sowie eine Analyse der erwarteten Endkunden stützt.

Or. en

Begründung

In der Checkliste wird genau dargelegt, zum Schutz gegen welche Risiken ein bestimmtes Produkt oder ein bestimmter Dienst entwickelt wurde, und entsprechende Cybersicherheitsmerkmale enthalten. Die Vertrauenswürdigkeitsstufe des Zertifikats nach Artikel 46 hängt von der Anzahl der Risiken ab, die das Zertifikat abdeckt. Die Checkliste wird dazu beitragen, die Herangehensweise in Abhängigkeit vom Produkt oder Dienst zu differenzieren, die von einem kleinen, privaten IoT-Gerät bis zu einer komplexen Anlagenverwaltung in kritischen Bereichen reichen.

Änderungsantrag 248

Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung

Artikel 44 – Absatz 3

Vorschlag der Kommission

3. **Die** ENISA **legt** der Kommission das nach Absatz 2 ausgearbeitete mögliche **europäische System für die Cybersicherheitszertifizierung** vor.

Geänderter Text

3. **Nach der Zustimmung der Gruppe zum möglichen europäischen System für die Cybersicherheitszertifizierung legt die ENISA nach Konsultation der Ständigen Gruppe der Interessenträger** der Kommission das nach Absatz 2 ausgearbeitete mögliche System vor.

Or. en

Änderungsantrag 249

Mylène Troszczyński

Vorschlag für eine Verordnung

Artikel 44 – Absatz 3

Vorschlag der Kommission

3. Die ENISA legt der Kommission das nach Absatz 2 ausgearbeitete **mögliche** europäische System für die Cybersicherheitszertifizierung vor.

Geänderter Text

3. Die ENISA legt der Kommission das nach Absatz 2 ausgearbeitete **und am Ende von den Mitgliedstaaten angenommene** europäische System für die Cybersicherheitszertifizierung vor.

Or. fr

Änderungsantrag 250
Anneleen Van Bossuyt, Daniel Dalton

Vorschlag für eine Verordnung
Artikel 44 – Absatz 4

Vorschlag der Kommission

4. *Auf der Grundlage des* von der ENISA ausgearbeiteten möglichen Systems kann die Kommission nach Artikel 55 Absatz 1 Durchführungsrechtsakte erlassen, in denen für IKT-Produkte und -Dienste, die die Anforderungen der Artikel 45, 46 und 47 erfüllen, europäische Systeme für die Cybersicherheitszertifizierung festgelegt werden.

Geänderter Text

4. *Die Kommission konsultiert alle in Frage kommenden Interessenträger zu dem* von der ENISA ausgearbeiteten möglichen System *und bewertet dessen Eignung für die Erreichung der Ziele des Auftrags und ob das System zu einem hohen Grad an Schutz für Verbraucher und Endnutzer sowie einer europäischen Wettbewerbsfähigkeit beiträgt. Nach der Konsultation und Bewertung* kann die Kommission nach Artikel 55 der 1 Durchführungsrechtsakte erlassen, in denen für IKT-Produkte und -Dienste, die die Anforderungen der Artikel 45, 46 und 47 erfüllen, europäische Systeme für die Cybersicherheitszertifizierung festgelegt werden.

Or. en

Änderungsantrag 251
Nicola Danti, Maria Grapini, Sergio Gutiérrez Prieto, Lucy Anderson, Arndt Kohn, Pina Picierno, Marc Tarabella, Christel Schaldemose

Vorschlag für eine Verordnung
Artikel 44 – Absatz 4

Vorschlag der Kommission

4. *Auf der Grundlage des von der ENISA ausgearbeiteten möglichen Systems kann die* Kommission nach Artikel 55 *Absatz 1* *Durchführungsrechtsakte erlassen, in denen* für IKT-Produkte und -Dienste, die die Anforderungen der Artikel 45, 46 und 47 erfüllen, *europäische Systeme für die Cybersicherheitszertifizierung festgelegt werden.*

Geänderter Text

4. *Die Kommission ist* nach Artikel 55a *befugt, für die Einrichtung europäischer Systeme für die Cybersicherheitszertifizierung* für IKT-Produkte und -Dienste, die die Anforderungen der Artikel 45, 46 und 47 erfüllen, *delegierte Rechtsakte zu erlassen. Beim Erlass solcher delegierten Rechtsakte stützt die Kommission die Systeme für die*

Cybersicherheitszertifizierung für IKT-Produkte und -Dienste auf entsprechende von der ENISA vorgeschlagene mögliche Systeme.

Or. en

Begründung

Da die Kommission eine bedeutende Zahl an Regeln zu Fragen wie dem Anwendungsbereich jedes Zertifizierungssystems, geltenden Anforderungen, Überwachungsvorschriften und so weiter festzulegen hat, ist es juristisch zutreffender, Zertifizierungssysteme durch delegierte Rechtsakte zu erlassen.

Änderungsantrag 252

Jan Philipp Albrecht

im Namen der Verts/ALE-Fraktion

Vorschlag für eine Verordnung

Artikel 44 – Absatz 4

Vorschlag der Kommission

4. Auf der Grundlage des von der ENISA ausgearbeiteten möglichen Systems kann die Kommission nach Artikel 55 Absatz 1 Durchführungsrechtsakte erlassen, in denen für IKT-Produkte und -Dienste, die die Anforderungen der Artikel 45, 46 und 47 erfüllen, europäische Systeme für die Cybersicherheitszertifizierung festgelegt werden.

Geänderter Text

4. Auf der Grundlage des von der ENISA ausgearbeiteten möglichen Systems kann die Kommission nach Artikel 55 Absatz 1 Durchführungsrechtsakte erlassen, in denen für IKT-Produkte und -Dienste, die die Anforderungen der Artikel 45, 46 und 47 erfüllen, europäische Systeme für die Cybersicherheitszertifizierung festgelegt werden. **Die Kommission kann vor dem Europäischen Datenschutzausschuss konsultieren und dessen Standpunkt berücksichtigen.**

Or. en

Begründung

Dies geht auf die Stellungnahme des EDSB zurück. Mit dieser Änderung wird dafür gesorgt, dass die Zertifizierungen, die im Zusammenhang mit dem europäischen Rahmen für die Cybersicherheitszertifizierung und der Datenschutz-Grundverordnung vorgenommen werden, kohärent sind.

Änderungsantrag 253
Mylène Troszczyński

Vorschlag für eine Verordnung
Artikel 44 – Absatz 4

Vorschlag der Kommission

4. Auf der Grundlage des von der ENISA **ausgearbeiteten möglichen Systems** kann die Kommission nach Artikel 55 Absatz 2 Durchführungsrechtsakte erlassen, in denen für IKT-Produkte und -Dienste, die die Anforderungen der Artikel 45, 46 und 47 erfüllen, europäische Systeme für die Cybersicherheitszertifizierung festgelegt werden.

Geänderter Text

4. Auf der Grundlage des von der ENISA **vorgelegten und von den Mitgliedstaaten angenommenen Zertifizierungssystems** kann die Kommission **dann** nach Artikel 55 Absatz 2 Durchführungsrechtsakte erlassen, in denen für IKT-Produkte und -Dienste, die die Anforderungen der Artikel 45, 46 und 47 erfüllen, europäische Systeme für die Cybersicherheitszertifizierung festgelegt werden.

Or. fr

Änderungsantrag 254
Roberta Metsola, Eva Maydell, Lara Comi, Carlos Coelho

Vorschlag für eine Verordnung
Artikel 44 – Absatz 4

Vorschlag der Kommission

4. Auf der Grundlage des von der ENISA ausgearbeiteten möglichen Systems kann die Kommission nach Artikel 55 Absatz 1 Durchführungsrechtsakte erlassen, in denen für IKT-Produkte und -Dienste, die die Anforderungen der Artikel 45, 46 und 47 erfüllen, europäische Systeme für die Cybersicherheitszertifizierung festgelegt werden.

Geänderter Text

4. Auf der Grundlage des von der ENISA ausgearbeiteten möglichen Systems kann die Kommission nach Artikel 55 Absatz 1 Durchführungsrechtsakte erlassen, in denen für **IKT-Hardware- und Software-**Produkte und -Dienste, die die Anforderungen der Artikel 45, 46 und 47 erfüllen, europäische Systeme für die Cybersicherheitszertifizierung festgelegt werden.

Or. en

Änderungsantrag 255

Roberta Metsola, Eva Maydell, Lara Comi, Carlos Coelho

Vorschlag für eine Verordnung

Artikel 44 – Absatz 5

Vorschlag der Kommission

5. Die ENISA unterhält eine eigene Website, auf der sie über die europäischen Systeme für die Cybersicherheitszertifizierung informiert und für diese wirbt.

Geänderter Text

5. Die ENISA unterhält eine eigene Website, auf der sie über die europäischen Systeme für die Cybersicherheitszertifizierung ***sowie über mögliche Systeme für die Cybersicherheitszertifizierung in der Ausarbeitung*** informiert und für diese wirbt.

Or. en

Änderungsantrag 256

Andreas Schwab, Philippe Juvin

Vorschlag für eine Verordnung

Artikel 44 – Absatz 5 a (neu)

Vorschlag der Kommission

Geänderter Text

5a. Die ENISA benötigt eine Außenstelle in Brüssel, um die Arbeit an EU-Zertifizierungen sorgfältig überwachen und um für den Aufbau gemeinsamer europäischer Normen zu Cybersicherheit in engem Kontakt mit der Kommission und dem Parlament arbeiten zu können.

Or. en

Änderungsantrag 257

Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung

Artikel 44 a (neu)

Artikel 44a

Arbeitsprogramm

1. Nach Konsultation der Gruppe und der Ständigen Gruppe der Interessenträger erstellt die ENISA nach Genehmigung durch die Kommission und in jedem Fall bis zum... [sechs Monate nach dem Inkrafttreten dieser Verordnung] und danach alle zwei Jahre in Ergänzung zu oder als Teil seines allgemeinen Arbeitsprogramms einen Arbeitsplan für die Entwicklung europäischer Systeme für die Cybersicherheitszertifizierung, der öffentlich zugänglich gemacht wird.

Die Arbeitspläne enthalten für die zwei Folgejahre eine indikative Liste der Produkte, Prozesse und Dienste, für die eine Annahme europäischer Systeme für die Cybersicherheitszertifizierung als vorrangig eingestuft wird. Der Arbeitsplan wird nach Konsultation der Kommission, der Gruppe und der Ständigen Gruppe der Interessenträger durch die ENISA gegebenenfalls geändert, um unter anderem die Anforderungen des Binnenmarkts zu berücksichtigen.

Or. en

Änderungsantrag 258

Roberta Metsola, Eva Maydell, Lara Comi, Carlos Coelho

Vorschlag für eine Verordnung

Artikel 45 – Absatz 1 – Einleitung

Vorschlag der Kommission

Für die Cybersicherheitszertifizierung wird ein europäisches System konzipiert, das – soweit zutreffend – **den** folgenden Sicherheitszielen Rechnung trägt:

Geänderter Text

Für die Cybersicherheitszertifizierung wird ein europäisches System konzipiert, das – soweit zutreffend – **der** folgenden **nicht erschöpfenden Liste an** Sicherheitszielen

Rechnung trägt:

Or. en

Änderungsantrag 259
Anneleen Van Bossuyt, Daniel Dalton

Vorschlag für eine Verordnung
Artikel 45 – Absatz 1 – Einleitung

Vorschlag der Kommission

Für die Cybersicherheitszertifizierung wird ein europäisches System konzipiert, das – **soweit zutreffend** – den folgenden Sicherheitszielen Rechnung trägt:

Geänderter Text

Für die Cybersicherheitszertifizierung wird jedes europäische System derart konzipiert, dass es – **mindestens** – den folgenden Sicherheitszielen Rechnung trägt, **sofern diese relevant sind**:

Or. en

Änderungsantrag 260
Dita Charanzová

Vorschlag für eine Verordnung
Artikel 45 – Absatz 1 – Einleitung

Vorschlag der Kommission

Für die Cybersicherheitszertifizierung wird ein europäisches System konzipiert, **das** – soweit zutreffend – den folgenden Sicherheitszielen Rechnung trägt:

Geänderter Text

Für die Cybersicherheitszertifizierung wird ein europäisches System **so** konzipiert, **dass es** – soweit zutreffend – den folgenden Sicherheitszielen Rechnung trägt:

Or. en

Änderungsantrag 261
Philippe Juvin

Vorschlag für eine Verordnung
Artikel 45 – Absatz 1 – Einleitung

Vorschlag der Kommission

Für die Cybersicherheitszertifizierung wird ein europäisches System konzipiert, das – **soweit zutreffend** – den folgenden Sicherheitszielen Rechnung trägt:

Geänderter Text

Für die Cybersicherheitszertifizierung wird ein europäisches System konzipiert, das den folgenden Sicherheitszielen Rechnung trägt:

Or. fr

Änderungsantrag 262
Jiří Maštálka

Vorschlag für eine Verordnung
Artikel 45 – Absatz 1 – Buchstabe a

Vorschlag der Kommission

(a) Gespeicherte, übermittelte oder anderweitig verarbeitete Daten werden gegen eine zufällige oder unbefugte Speicherung, Verarbeitung oder Preisgabe sowie gegen einen zufälligen oder unbefugten Zugriff geschützt.

Geänderter Text

(a) **Vertraulichkeit** : Gespeicherte, übermittelte oder anderweitig verarbeitete Daten werden gegen eine zufällige oder unbefugte Speicherung, Verarbeitung oder Preisgabe sowie gegen einen zufälligen oder unbefugten Zugriff geschützt.

Or. en

Änderungsantrag 263
Jiří Maštálka

Vorschlag für eine Verordnung
Artikel 45 – Absatz 1 – Buchstabe b

Vorschlag der Kommission

(b) Gespeicherte, übermittelte oder anderweitig verarbeitete Daten werden gegen eine zufällige oder unbefugte Zerstörung, einen zufälligen Verlust oder eine zufällige Änderung geschützt.

Geänderter Text

(b) **Integrität** : Gespeicherte, übermittelte oder anderweitig verarbeitete Daten werden gegen eine zufällige oder unbefugte Zerstörung, einen zufälligen Verlust oder eine zufällige Änderung geschützt.

Or. en

Änderungsantrag 264
Jiří Maštálka

Vorschlag für eine Verordnung
Artikel 45 – Absatz 1 – Buchstabe c

Vorschlag der Kommission

Geänderter Text

(c) Es wird gewährleistet, dass befugte Personen, Programme oder Maschinen exklusiven Zugriff auf die Daten, Dienste oder Funktionen haben, zu denen sie Zugangsberechtigt sind. **entfällt**

Or. en

Änderungsantrag 265
Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Artikel 45 – Absatz 1 – Buchstabe c a (neu)

Vorschlag der Kommission

Geänderter Text

(ca) Geräte werden gegen Spoofing und andere Formen von Gerätemanipulation gesichert und geschützt.

Or. en

Änderungsantrag 266
Jiří Maštálka

Vorschlag für eine Verordnung
Artikel 45 – Absatz 1 – Buchstabe d

Vorschlag der Kommission

Geänderter Text

(d) Es wird protokolliert, welche Daten, Funktionen oder Dienste zu welchem Zeitpunkt von wem übermittelt bzw. genutzt worden sind. **entfällt**

Or. en

Änderungsantrag 267
Jiří Maštálka

Vorschlag für eine Verordnung
Artikel 45 – Absatz 1 – Buchstabe e

Vorschlag der Kommission

Geänderter Text

(e) Es wird gewährleistet, dass überprüft werden kann, auf welche Daten, Dienste oder Funktionen zu welchem Zeitpunkt und von wem zugegriffen wurde oder wer zu welchem Zeitpunkt Daten, Dienste oder Funktionen genutzt hat.

entfällt

Or. en

Änderungsantrag 268
Jiří Maštálka

Vorschlag für eine Verordnung
Artikel 45 – Absatz 1 – Buchstabe f

Vorschlag der Kommission

Geänderter Text

(f) Bei einem physischen oder technischen Sicherheitsvorfall werden die Daten, Dienste und Funktionen zeitnah wieder verfügbar gemacht und der Zugang zu ihnen zeitnah wieder hergestellt.

(f) Verfügbarkeit: Der Zugang berechtigter Nutzer zu Daten, Diensten und Funktionen wird gefördert.

Or. en

Änderungsantrag 269
Anneleen Van Bossuyt, Daniel Dalton

Vorschlag für eine Verordnung
Artikel 45 – Absatz 1 – Buchstabe g

Vorschlag der Kommission

Geänderter Text

(g) Es wird gewährleistet, dass IKT-Produkte und -Dienste mit aktueller Software, die keine bekannten Schwachstellen aufweist, bereitgestellt werden und mit Mechanismen für sichere Software-Updates ausgestattet sind.

(g) Es wird gewährleistet, dass IKT-Produkte und -Dienste mit aktueller Software, die keine bekannten, **für die durch das System vergebene Vertrauenswürdigkeitsstufe kritischen** Schwachstellen aufweist, bereitgestellt werden, **derart konzipiert und ausgeführt sind, dass sie die Einbeziehung oder Einführung von Schwachstellen effektiv einschränken** und mit Mechanismen für sichere Software-Updates ausgestattet sind.

Or. en

Änderungsantrag 270 Andreas Schwab

Vorschlag für eine Verordnung Artikel 45 – Absatz 1 – Buchstabe g

Vorschlag der Kommission

(g) Es wird gewährleistet, dass IKT-Produkte und -Dienste mit **aktueller Software**, die keine bekannten Schwachstellen **aufweist**, bereitgestellt werden und **mit Mechanismen für sichere Software-Updates ausgestattet sind**.

Geänderter Text

(g) Es wird gewährleistet, dass IKT-Produkte und -Dienste mit **Updates, Upgrades und Patches**, die keine bekannten Schwachstellen **aufweisen**, bereitgestellt werden und **die für den normalen Lebenszyklus des Produkts oder Dienstes angeboten werden müssen, um einen kontinuierlichen Schutz zu ermöglichen**.

Or. en

Änderungsantrag 271 Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung Artikel 45 – Absatz 1 – Buchstabe g

Vorschlag der Kommission

(g) Es wird gewährleistet, dass IKT-Produkte und -Dienste mit aktueller Software, die keine bekannten

Geänderter Text

(g) Es wird gewährleistet, dass IKT-Produkte und -Dienste mit aktueller Software **und Hardware**, die keine

Schwachstellen **aufweist**, bereitgestellt werden und mit Mechanismen für sichere Software-Updates ausgestattet sind.

bekannten Schwachstellen **aufweisen**, bereitgestellt werden und mit Mechanismen für sichere Software-Updates ausgestattet sind, **einschließlich automatischer Sicherheitsupdates**;

Or. en

Änderungsantrag 272

Roberta Metsola, Eva Maydell, Lara Comi, Pascal Arimont, Carlos Coelho

Vorschlag für eine Verordnung

Artikel 45 – Absatz 1 – Buchstabe g

Vorschlag der Kommission

(g) Es wird gewährleistet, dass **IKT-Produkte und -Dienste** mit aktueller Software, die keine bekannten Schwachstellen aufweist, bereitgestellt werden und mit Mechanismen für sichere Software-Updates ausgestattet sind.

Geänderter Text

(g) Es wird gewährleistet, dass **IKT-Hardware und Software-Produkte und -Dienste** mit aktueller Software, die keine bekannten Schwachstellen aufweist, bereitgestellt werden und mit Mechanismen für sichere Software-Updates ausgestattet sind.

Or. en

Änderungsantrag 273

Jiří Pospíšil

Vorschlag für eine Verordnung

Artikel 45 – Absatz 1 – Buchstabe g

Vorschlag der Kommission

g) Es wird gewährleistet, dass IKT-Produkte und -Dienste mit aktueller Software, die keine bekannten Schwachstellen aufweist, bereitgestellt werden und mit Mechanismen für sichere Software-Updates ausgestattet sind.

Geänderter Text

g) Es wird gewährleistet, dass IKT-Produkte und -Dienste mit aktueller Software, die keine bekannten Schwachstellen **oder Mängel** aufweist, bereitgestellt werden und mit Mechanismen für sichere Software-Updates ausgestattet sind.

Or. cs

Änderungsantrag 274
Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Artikel 45 – Absatz 1 – Buchstabe g a (neu)

Vorschlag der Kommission

Geänderter Text

(ga) Es wird gewährleistet, dass IKT-Produkte und -Dienste in Übereinstimmung mit entsprechenden Sicherheitsstandards und -richtlinien entwickelt und betrieben werden und dass das höchste angemessene Maß an Cybersicherheit und Datenschutz von Anfang an standardmäßig in Produkten, Diensten und Prozessen eingebaut wird.

Or. en

Änderungsantrag 275
Catherine Stihler, Liisa Jaakonsaari, Christel Schaldemose, Arndt Kohn, Lucy Anderson

Vorschlag für eine Verordnung
Artikel 45 – Absatz 1 – Buchstabe g a (neu)

Vorschlag der Kommission

Geänderter Text

(ga) Es wird gewährleistet, dass IKT-Produkte und -Dienste gemäß dem Grundsatz der Sicherheit als Designkriterium ausgehend von einem risikobasierten Ansatz je nach Kontext und Ernsthaftigkeit der Lage gemäß Artikel 46 entwickelt werden.

Or. en

Änderungsantrag 276
Roberta Metsola, Eva Maydell, Lara Comi, Carlos Coelho

Vorschlag für eine Verordnung
Artikel 46 – Überschrift

Vorschlag der Kommission

Geänderter Text

Vertrauenswürdigkeitsstufen der europäischen Systeme für die Cybersicherheitszertifizierung

Risikobasierte
Vertrauenswürdigkeitsstufen der europäischen Systeme für die Cybersicherheitszertifizierung

Or. en

Änderungsantrag 277
Andreas Schwab, Philippe Juvin

Vorschlag für eine Verordnung
Artikel 46 – Überschrift

Vorschlag der Kommission

Geänderter Text

Vertrauenswürdigkeitsstufen der europäischen Systeme für die Cybersicherheitszertifizierung

Sicherheitsanforderungen der europäischen Systeme für die Cybersicherheitszertifizierung

Or. en

Änderungsantrag 278
Anneleen Van Bossuyt, Daniel Dalton

Vorschlag für eine Verordnung
Artikel 46 – Absatz 1

Vorschlag der Kommission

Geänderter Text

1. Ein europäisches System für die Cybersicherheitszertifizierung kann für auf der Grundlage dieses Systems zertifizierte IKT-Produkte und -Dienste ***eine oder mehrere der*** Vertrauenswürdigkeitsstufen „***niedrig***“, „***mittel***“ bzw. „***hoch***“ angeben.

1. Ein europäisches System für die Cybersicherheitszertifizierung kann für auf der Grundlage dieses Systems zertifizierte IKT-Produkte und -Dienste ***unterschiedliche*** Vertrauenswürdigkeitsstufen angeben. ***Diese Stufen werden auf der Grundlage des Maßes an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes unterschieden und durch die Bezugnahme auf die diesbezüglichen technischen Normen und Verfahren einschließlich technischer***

Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet.

Or. en

Änderungsantrag 279
Antanas Guoga

Vorschlag für eine Verordnung
Artikel 46 – Absatz 1

Vorschlag der Kommission

1. *Ein europäisches System für die Cybersicherheitszertifizierung **kann für auf der Grundlage dieses Systems zertifizierte IKT-Produkte und -Dienste eine oder mehrere der Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ bzw. „hoch“ angeben.***

Geänderter Text

1. ***Nach Konsultation der in Frage kommenden Interessenträger bestimmt und entwickelt die ENISA Vertrauenswürdigkeitsstufen, die in europäischen Systemen für die Cybersicherheitszertifizierung **angegeben werden.*****

Or. en

Änderungsantrag 280
Jiří Maštálka

Vorschlag für eine Verordnung
Artikel 46 – Absatz 1

Vorschlag der Kommission

1. Ein europäisches System für die Cybersicherheitszertifizierung kann ***für auf der Grundlage dieses Systems zertifizierte IKT-Produkte und -Dienste*** eine oder mehrere ***der Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ bzw. „hoch“*** angeben.

Geänderter Text

1. Ein europäisches System für die Cybersicherheitszertifizierung kann eine oder mehrere ***Vertrauenswürdigkeitsanforderungen, beruhend auf den Risiken und Gefahren, die von dem Kontext bestimmt werden, in dem das Produkt, der Prozess oder der Dienst genutzt werden,*** angeben.

Or. en

Änderungsantrag 281
Andreas Schwab, Philippe Juvin

Vorschlag für eine Verordnung
Artikel 46 – Absatz 1

Vorschlag der Kommission

1. Ein europäisches System für die Cybersicherheitszertifizierung kann für auf der Grundlage dieses Systems zertifizierte IKT-Produkte und -Dienste eine oder mehrere *der Vertrauenswürdigkeitsstufen* „niedrig“, „mittel“ bzw. „hoch“ angeben.

Geänderter Text

1. Ein europäisches System für die Cybersicherheitszertifizierung kann für auf der Grundlage dieses Systems zertifizierte IKT-Produkte und -Dienste eine oder mehrere *der Sicherheitsanforderungen* „niedrig“, „mittel“ bzw. „hoch“ angeben. ***Die Sicherheitsanforderungen werden ausgehend von einem risikobasierten Ansatz festgelegt, wobei die beabsichtigte Nutzung des IKT-Produkts oder -Dienstes berücksichtigt wird.***

Or. en

Änderungsantrag 282
Nicola Danti, Evelyne Gebhardt, Maria Grapini, Sergio Gutiérrez Prieto, Lucy Anderson, Arndt Kohn, Kerstin Westphal, Pina Picierno, Marc Tarabella, Christel Schaldemose

Vorschlag für eine Verordnung
Artikel 46 – Absatz 1

Vorschlag der Kommission

1. ***Ein europäisches*** System für die Cybersicherheitszertifizierung kann für auf der Grundlage dieses Systems zertifizierte IKT-Produkte und -Dienste eine oder mehrere der Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ bzw. „hoch“ angeben.

Geänderter Text

1. ***Jedes europäische*** System für die Cybersicherheitszertifizierung kann für auf der Grundlage dieses Systems zertifizierte IKT-Produkte und -Dienste eine oder mehrere der Vertrauenswürdigkeitsstufen „funktional sicher“, „ziemlich sicher“ bzw. „äußerst sicher“ angeben, ***unter Berücksichtigung unter anderem ihrer bestimmungsgemäßen Verwendung und der ihnen innewohnenden Risiken.***

Or. en

Begründung

Die Vertrauenswürdigkeitsstufe jedes Systems für die Cybersicherheitszertifizierung sollte die Verwendung oder die Bestimmung des IKT-Produkts und -Dienstes und das ihnen innewohnende Risiko berücksichtigen und nicht das IKT-Produkt und den -Dienst als solches(n).

Änderungsantrag 283

Dita Charanzová

Vorschlag für eine Verordnung

Artikel 46 – Absatz 1

Vorschlag der Kommission

1. **Ein europäisches** System für die Cybersicherheitszertifizierung kann für auf der Grundlage dieses Systems **zertifizierte IKT-Produkte und -Dienste** eine oder mehrere der Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ bzw. „hoch“ angeben.

Geänderter Text

1. **Jedes europäische** System für die Cybersicherheitszertifizierung kann für auf der Grundlage dieses Systems **ausgestellte Cybersicherheitszertifikate** eine oder mehrere der Vertrauenswürdigkeitsstufen – „funktional sicher“, „ziemlich sicher“ bzw. „äußerst sicher“ oder eine **Kombination daraus** – angeben, **unter Berücksichtigung unter anderem ihrer bestimmungsgemäßen Verwendung.**

Or. en

Änderungsantrag 284

Roberta Metsola, Lara Comi

Vorschlag für eine Verordnung

Artikel 46 – Absatz 1

Vorschlag der Kommission

1. Ein europäisches System für die Cybersicherheitszertifizierung kann für auf der Grundlage dieses Systems zertifizierte **IKT-Produkte und -Dienste** eine oder mehrere der Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ bzw. „hoch“ angeben.

Geänderter Text

1. Ein europäisches System für die Cybersicherheitszertifizierung kann für auf der Grundlage dieses Systems zertifizierte IKT-Produkte und -Dienste eine oder mehrere der Vertrauenswürdigkeitsstufen „**grundlegend**“, „mittel“ bzw. „hoch“ angeben.

Or. en

Änderungsantrag 285
Jiří Pospíšil

Vorschlag für eine Verordnung
Artikel 46 – Absatz 1

Vorschlag der Kommission

1. Ein europäisches System für die Cybersicherheitszertifizierung kann für auf der Grundlage dieses Systems zertifizierte IKT-Produkte und -Dienste eine oder mehrere der Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ bzw. „hoch“ angeben.

Geänderter Text

(Betrifft nicht die deutsche Fassung.)

Or. cs

Änderungsantrag 286

Nicola Danti, Maria Grapini, Sergio Gutiérrez Prieto, Lucy Anderson, Arndt Kohn, Catherine Stihler, Pina Picierno, Marc Tarabella, Christel Schaldemose

Vorschlag für eine Verordnung
Artikel 46 – Absatz 1 a (neu)

Vorschlag der Kommission

1a. Jedes System muss die Beurteilungsmethodik bzw. das Bewertungsverfahren angeben, die bzw. das für das Ausstellen von Zertifikaten auf jeder Vertrauenswürdigkeitsstufe zu befolgen ist, abhängig von der bestimmungsgemäßen Verwendung der IKT-Produkte und Dienste und den ihnen innewohnenden Risiken nach diesem System.

Geänderter Text

Or. en

Begründung

Um eine Fragmentierung in den EU-Mitgliedstaaten zu vermeiden, sollte jede Vertrauenswürdigkeitsstufe mit einer Beurteilungsmethodik oder einem Bewertungsverfahren verknüpft sein.

Änderungsantrag 287

Roberta Metsola, Lara Comi, Andreas Schwab, Jiří Pospíšil

Vorschlag für eine Verordnung

Artikel 46 – Absatz 1 a (neu)

Vorschlag der Kommission

Geänderter Text

1a. Ein europäisches System für die Cybersicherheitszertifizierung muss angeben, ob eine Konformitäts-Eigenerklärung zulässig oder ob eine Beurteilung durch Dritte zwingend erforderlich ist.

Or. en

Änderungsantrag 288

Antanas Guoga

Vorschlag für eine Verordnung

Artikel 46 – Absatz 2

Vorschlag der Kommission

Geänderter Text

2. Die Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ bzw. „hoch“ erfüllen jeweils folgende Kriterien:

entfällt

(a) Die Vertrauenswürdigkeitsstufe „niedrig“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein begrenztes Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

(b) Die Vertrauenswürdigkeitsstufe „mittel“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein mittleres Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

(c) Die Vertrauenswürdigkeitsstufe „hoch“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein höheres Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt als Zertifikate mit der Vertrauenswürdigkeitsstufe „mittel“ und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

Or. en

Geänderter Text 289
Anneleen Van Bossuyt, Daniel Dalton

Vorschlag für eine Verordnung
Artikel 46 – Absatz 2

Vorschlag der Kommission

Geänderter Text

2. Die Vertrauenswürdigkeitsstufen **entfällt**

„niedrig“, „mittel“ bzw. „hoch“ erfüllen jeweils folgende Kriterien:

(a) Die Vertrauenswürdigkeitsstufe „niedrig“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein begrenztes Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

(b) Die Vertrauenswürdigkeitsstufe „mittel“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein mittleres Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

(c) Die Vertrauenswürdigkeitsstufe „hoch“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein höheres Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt als Zertifikate mit der Vertrauenswürdigkeitsstufe „mittel“ und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren

einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

Or. en

Änderungsantrag 290
Jiří Maštálka

Vorschlag für eine Verordnung
Artikel 46 – Absatz 2 – Einleitung

Vorschlag der Kommission

2. Die Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ bzw. „hoch“ erfüllen jeweils folgende Kriterien:

Geänderter Text

2. Ein europäisches System für die Cybersicherheitszertifizierung muss angeben, ob eine Konformitäts-Eigenerklärung zulässig ist und/oder ob eine Beurteilung durch Dritte zwingend erforderlich ist.

Or. en

Begründung

Die Systeme für die Cybersicherheitszertifizierung sollten je nach Risikograd und Nutzung des Produkts, Dienstes oder Prozesses flexibel sein. Es muss möglich sein, auf ein sich schnell wandelndes Umfeld reagieren zu können.

Änderungsantrag 291
Roberta Metsola, Eva Maydell, Lara Comi

Vorschlag für eine Verordnung
Artikel 46 – Absatz 2 – Einleitung

Vorschlag der Kommission

2. Die Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ bzw. „hoch“ erfüllen jeweils folgende Kriterien:

Geänderter Text

2. Die **risikobasierten** Vertrauenswürdigkeitsstufen „**grundlegend**“, „mittel“ bzw. „hoch“ erfüllen jeweils folgende Kriterien:

Or. en

Änderungsantrag 292
Andreas Schwab, Philippe Juvin

Vorschlag für eine Verordnung
Artikel 46 – Absatz 2 – Einleitung

Vorschlag der Kommission

2. Die **Vertrauenswürdigkeitsstufen** „niedrig“, „mittel“ bzw. „hoch“ erfüllen jeweils folgende Kriterien:

Geänderter Text

2. Die **Sicherheitsanforderungen** „niedrig“, „mittel“ bzw. „hoch“ erfüllen jeweils folgende Kriterien:

Or. en

Änderungsantrag 293
Jiří Maštálka

Vorschlag für eine Verordnung
Artikel 46 – Absatz 2 – Buchstabe a

Vorschlag der Kommission

(a) Die Vertrauenswürdigkeitsstufe „niedrig“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestellttes Zertifikat, das ein begrenztes Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

entfällt

Geänderter Text

Or. en

Änderungsantrag 294
Antanas Guoga

**Vorschlag für eine Verordnung
Artikel 46 – Absatz 2 – Buchstabe a**

Vorschlag der Kommission

Geänderter Text

(a) Die Vertrauenswürdigkeitsstufe „niedrig“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein begrenztes Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

entfällt

Or. en

Änderungsantrag 295

Arndt Kohn, Evelyne Gebhardt, Kerstin Westphal, Pina Picierno, Christel Schaldemose

**Vorschlag für eine Verordnung
Artikel 46 – Absatz 2 – Buchstabe a**

Vorschlag der Kommission

Geänderter Text

(a) Die Vertrauenswürdigkeitsstufe „niedrig“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein begrenztes Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der

(a) Die Vertrauenswürdigkeitsstufe „funktional sicher“ bezieht sich auf ein geringes Risiko eines IKT-Produkts und -Dienstes. Ein geringes Risiko besteht, wenn ein Angriff auf das IKT-Produkt und den IKT-Dienst weder die Vertraulichkeit, Integrität, Verfügbarkeit, Privatsphäre oder andere wichtige Zielsetzungen noch die Gesundheit von Nutzern oder Dritten, die Umwelt, andere wichtige Rechtsgüter oder kritische Infrastrukturen und die sie unterstützenden Systeme oder Produkte beeinträchtigt.

**Gefahr von Cybersicherheitsvorfällen
besteht – gekennzeichnet ist.**

Or. en

**Änderungsantrag 296
Dita Charanzová**

**Vorschlag für eine Verordnung
Artikel 46 – Absatz 2 – Buchstabe a**

Vorschlag der Kommission

(a) Die Vertrauenswürdigkeitsstufe „**niedrig**“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein **begrenztes** Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

Geänderter Text

(a) Die Vertrauenswürdigkeitsstufe „**funktional sicher**“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein **angemessenes** Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist. **Wenn ein europäisches System für die Cybersicherheitszertifizierung die Zertifizierung eines Cybersicherheitsprozesses durch einen Hersteller einschließt, kann diese Zertifizierung eines Cybersicherheitsprozesses die Erteilung einer Genehmigung für eine Eigenerklärung des Herstellers zur Konformität von IKT-Produkten oder -Dienstern mit der Vertrauenswürdigkeitsstufe „funktional sicher“ einschließen.**

Or. en

Änderungsantrag 297

Roberta Metsola, Lara Comi

**Vorschlag für eine Verordnung
Artikel 46 – Absatz 2 – Buchstabe a**

Vorschlag der Kommission

(a) Die Vertrauenswürdigkeitsstufe „**niedrig**“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein **begrenzt**es Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

Geänderter Text

(a) Die **risikobasierte** Vertrauenswürdigkeitsstufe „**grundlegend**“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein **notwendiges Mindestmaß** an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes **und deren Sicherheit bei häufigen, überwiegend Konsumgüter betreffenden Bedrohungen der Cybersicherheit** vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

Or. en

**Änderungsantrag 298
Andreas Schwab, Philippe Juvin**

**Vorschlag für eine Verordnung
Artikel 46 – Absatz 2 – Buchstabe a**

Vorschlag der Kommission

(a) Die **Vertrauenswürdigkeitsstufe** „niedrig“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein **begrenzt**es Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf

Geänderter Text

(a) Die **Sicherheitsanforderung** „niedrig“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein **begrenzt**es Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf

die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

Or. en

Änderungsantrag 299
Jiří Maštálka

Vorschlag für eine Verordnung
Artikel 46 – Absatz 2 – Buchstabe b

Vorschlag der Kommission

Geänderter Text

(b) Die Vertrauenswürdigkeitsstufe „mittel“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein mittleres Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

entfällt

Or. en

Änderungsantrag 300
Antanas Guoga

Vorschlag für eine Verordnung
Artikel 46 – Absatz 2 – Buchstabe b

Vorschlag der Kommission

Geänderter Text

(b) Die Vertrauenswürdigkeitsstufe

entfällt

„mittel“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein mittleres Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

Or. en

Änderungsantrag 301

Arndt Kohn, Evelyne Gebhardt, Kerstin Westphal, Pina Picierno, Christel Schaldemose

Vorschlag für eine Verordnung

Artikel 46 – Absatz 2 – Buchstabe b

Vorschlag der Kommission

(b) Die Vertrauenswürdigkeitsstufe „mittel“ bezieht sich auf ein **im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein mittleres Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.**

Geänderter Text

(b) Die Vertrauenswürdigkeitsstufe „**ziemlich sicher**“ bezieht sich auf ein **höheres Risiko eines IKT-Produkts und -Dienstes. Ein höheres Risiko besteht, wenn ein Angriff auf das IKT-Produkt und den IKT-Dienst die Vertraulichkeit, Integrität, Verfügbarkeit, Privatsphäre oder andere wichtige Zielsetzungen beeinträchtigt und Auswirkungen auf die Gesundheit von Nutzern oder Dritten, die Umwelt, andere wichtige Rechtsgüter oder kritische Infrastrukturen und die sie unterstützenden Systeme oder Produkte hat.**

Or. en

Änderungsantrag 302

Roberta Metsola, Eva Maydell, Lara Comi, Carlos Coelho

Vorschlag für eine Verordnung

Artikel 46 – Absatz 2 – Buchstabe b

Vorschlag der Kommission

(b) Die Vertrauenswürdigkeitsstufe „mittel“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein mittleres Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

Geänderter Text

(b) Die **risikobasierte** Vertrauenswürdigkeitsstufe „mittel“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein mittleres Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen, **die im Allgemeinen auf Branchenebene angewandt werden** – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

Or. en

Änderungsantrag 303

Andreas Schwab, Philippe Juvin

Vorschlag für eine Verordnung

Artikel 46 – Absatz 2 – Buchstabe b

Vorschlag der Kommission

(b) Die **Vertrauenswürdigkeitsstufe** „mittel“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein mittleres Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen

Geänderter Text

(b) Die **Sicherheitsanforderung** „mittel“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein mittleres Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt und durch die Bezugnahme auf die diesbezüglichen technischen

Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

Or. en

Änderungsantrag 304
Antanas Guoga

Vorschlag für eine Verordnung
Artikel 46 – Absatz 2 – Buchstabe c

Vorschlag der Kommission

Geänderter Text

(c) Die Vertrauenswürdigkeitsstufe „hoch“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein höheres Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt als Zertifikate mit der Vertrauenswürdigkeitsstufe „mittel“ und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

entfällt

Or. en

Änderungsantrag 305
Jiří Maštálka

Vorschlag für eine Verordnung
Artikel 46 – Absatz 2 – Buchstabe c

Vorschlag der Kommission

Geänderter Text

(c) Die Vertrauenswürdigkeitsstufe „hoch“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein höheres Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt als Zertifikate mit der Vertrauenswürdigkeitsstufe „mittel“ und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

entfällt

Or. en

Änderungsantrag 306

Arndt Kohn, Evelyn Gebhardt, Kerstin Westphal, Pina Picierno, Christel Schaldemose

Vorschlag für eine Verordnung

Artikel 46 – Absatz 2 – Buchstabe c

Vorschlag der Kommission

Geänderter Text

(c) Die Vertrauenswürdigkeitsstufe „hoch“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein höheres Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt als Zertifikate mit der Vertrauenswürdigkeitsstufe „mittel“ und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen

(c) Die Vertrauenswürdigkeitsstufe „äußerst sicher“ bezieht sich auf ein hohes Risiko eines IKT-Produkts und -Dienstes. Ein hohes Risiko besteht, wenn ein Angriff auf ein IKT-Produkt und einen IKT-Dienst die Vertraulichkeit, Integrität, Verfügbarkeit, Privatsphäre oder andere wichtige Zielsetzungen beeinträchtigt und die nationale Souveränität oder öffentliche Sicherheit von Staaten maßgeblich gefährdet.

besteht – gekennzeichnet ist.

Or. en

Änderungsantrag 307

Liisa Jaakonsaari, Christel Schaldemose, Lucy Anderson

Vorschlag für eine Verordnung

Artikel 46 – Absatz 2 – Buchstabe c

Vorschlag der Kommission

(c) Die Vertrauenswürdigkeitsstufe „hoch“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein höheres Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt als Zertifikate mit der Vertrauenswürdigkeitsstufe „mittel“ und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

Geänderter Text

(c) Die Vertrauenswürdigkeitsstufe „hoch“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein höheres Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt als Zertifikate mit der Vertrauenswürdigkeitsstufe „mittel“ und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist. ***Diese Vertrauenswürdigkeitsstufe darf keine absolute Sicherheit suggerieren, um den Endnutzer nicht irrezuführen.***

Or. en

Änderungsantrag 308

Andreas Schwab, Philippe Juvin

Vorschlag für eine Verordnung

Artikel 46 – Absatz 2 – Buchstabe c

Vorschlag der Kommission

(c) Die *Vertrauenswürdigkeitsstufe* „hoch“ bezieht sich auf ein im Rahmen

Geänderter Text

(c) Die ***Sicherheitsanforderung*** „hoch“ bezieht sich auf ein im Rahmen

einer europäischen
Cybersicherheitszertifizierung ausgestelltes
Zertifikat, das ein höheres Maß an
Vertrauen in die beanspruchten oder
behaupteten Cybersicherheitseigenschaften
eines IKT-Produkts oder -Dienstes
vermittelt als Zertifikate mit der
Vertrauenswürdigkeitsstufe „mittel“ und
durch die Bezugnahme auf die
diesbezüglichen technischen
Spezifikationen, Normen und Verfahren
einschließlich technischer Prüfungen –
deren Zweck in der Minderung der Gefahr
von Cybersicherheitsvorfällen besteht –
gekennzeichnet ist.

einer europäischen
Cybersicherheitszertifizierung ausgestelltes
Zertifikat, das ein höheres Maß an
Vertrauen in die beanspruchten oder
behaupteten Cybersicherheitseigenschaften
eines IKT-Produkts oder -Dienstes
vermittelt als Zertifikate mit der
Sicherheitsanforderung „mittel“ und
durch die Bezugnahme auf die
diesbezüglichen technischen
Spezifikationen, Normen und Verfahren
einschließlich technischer Prüfungen –
deren Zweck in der Minderung der Gefahr
von Cybersicherheitsvorfällen besteht –
gekennzeichnet ist. **Dies findet
insbesondere Anwendung auf Produkte
und Dienste in kritischen Infrastrukturen.**

Or. en

Änderungsantrag 309

Roberta Metsola, Eva Maydell, Lara Comi, Carlos Coelho

Vorschlag für eine Verordnung

Artikel 46 – Absatz 2 – Buchstabe c

Vorschlag der Kommission

(c) Die Vertrauenswürdigkeitsstufe
„hoch“ bezieht sich auf ein im Rahmen
einer europäischen
Cybersicherheitszertifizierung ausgestelltes
Zertifikat, das ein höheres Maß an
Vertrauen in die beanspruchten oder
behaupteten Cybersicherheitseigenschaften
eines IKT-Produkts oder -Dienstes
vermittelt als Zertifikate mit der
Vertrauenswürdigkeitsstufe „mittel“ und
durch die Bezugnahme auf die
diesbezüglichen technischen
Spezifikationen, Normen und Verfahren
einschließlich technischer Prüfungen –
deren Zweck in der Minderung der Gefahr
von Cybersicherheitsvorfällen besteht –
gekennzeichnet ist.

Geänderter Text

(c) Die **risikobasierte**
Vertrauenswürdigkeitsstufe „hoch“ bezieht
sich auf ein im Rahmen einer europäischen
Cybersicherheitszertifizierung ausgestelltes
Zertifikat, das ein höheres Maß an
Vertrauen in die beanspruchten oder
behaupteten Cybersicherheitseigenschaften
eines IKT-Produkts oder -Dienstes
vermittelt als Zertifikate mit der
Vertrauenswürdigkeitsstufe „mittel“ und
durch die Bezugnahme auf die
diesbezüglichen technischen
Spezifikationen, Normen und Verfahren
einschließlich technischer Prüfungen, **die
im Allgemeinen auf Branchenebene
angewandt werden** – deren Zweck in der
Minderung der Gefahr von
Cybersicherheitsvorfällen besteht –

gekennzeichnet ist.

Or. en

Änderungsantrag 310

Dita Charanzová

Vorschlag für eine Verordnung

Artikel 46 – Absatz 2 – Buchstabe c

Vorschlag der Kommission

(c) Die Vertrauenswürdigkeitsstufe „**hoch**“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein höheres Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt als Zertifikate mit der Vertrauenswürdigkeitsstufe „**mittel**“ und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

Geänderter Text

(c) Die Vertrauenswürdigkeitsstufe „**äußerst sicher**“ bezieht sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein höheres Maß an Vertrauen in die beanspruchten oder behaupteten Cybersicherheitseigenschaften eines IKT-Produkts oder -Dienstes vermittelt als Zertifikate mit der Vertrauenswürdigkeitsstufe „**ziemlich sicher**“ und durch die Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist.

Or. en

Änderungsantrag 311

Roberta Metsola, Lara Comi, Carlos Coelho

Vorschlag für eine Verordnung

Artikel 46 – Absatz 2 a (neu)

Vorschlag der Kommission

Geänderter Text

2a. Die risikobasierte Vertrauenswürdigkeitsstufe für ein mögliches europäisches System für die Cybersicherheitszertifizierung wird auf der Grundlage der Checkliste nach

Artikel 44 Absatz 2 und der Verfügbarkeit von Cybersicherheitsmaßnahmen zur Bekämpfung dieser Risiken in den IKT-Hardware- und Softwareprodukten und -diensten festgelegt, für die das Zertifizierungssystem gilt.

Or. en

Begründung

In der Checkliste wird dargelegt, zum Schutz gegen welche Risiken ein bestimmtes Produkt oder ein bestimmter Dienst entwickelt wurde, und entsprechende Cybersicherheitsmerkmale enthalten. Die Vertrauenswürdigkeitsstufe des Zertifikats nach Artikel 46 hängt von der Anzahl der Risiken ab, die das Zertifikat abdeckt. Die Checkliste wird dazu beitragen, die Herangehensweise in Abhängigkeit vom Produkt oder Dienst zu differenzieren, die von einem kleinen, privaten IoT-Gerät bis zu einer komplexen Anlagenverwaltung in kritischen Bereichen reichen.

Änderungsantrag 312

Philippe Juvin, Andreas Schwab

Vorschlag für eine Verordnung

Artikel 46 – Absatz 2 a (neu)

Vorschlag der Kommission

Geänderter Text

2a. Im Hinblick auf mittlere und hohe Vertrauenswürdigkeitsstufen können die nationalen Konformitätsbewertungsstellen die Methode des „ethischen Hackens“ anwenden.

Or. fr

Änderungsantrag 313

Roberta Metsola, Lara Comi, Antonio López-Istúriz White, Carlos Coelho

Vorschlag für eine Verordnung

Artikel 46 – Absatz 2 b (neu)

Vorschlag der Kommission

Geänderter Text

2b. Die für die risikobasierte

Vertrauenswürdigkeitsstufe „grundlegend“ in Artikel 46 Absatz 2 festgelegten Merkmale sind die Mindestmaßnahmen für Cybersicherheit, die für Konsumgüter vertretbar sind. Die für die risikobasierten Vertrauenswürdigkeitsstufen „mittel“ und „hoch“ festgelegten Merkmale sind die Mindestmaßnahmen für Cybersicherheit, die für auf Branchenebene angewandte IKT-Software und Hardware-Produkte und -Dienste vertretbar sind. Diese allgemeinen Merkmale sollten ENISA nicht davon abhalten, nach Konsultation der Mitgliedstaaten und der Ständigen Gruppe der Interessenträger und einer gründlichen Bewertung eine höhere risikobasierte Vertrauenswürdigkeitsstufe als die zwingend erforderliche auszuwählen.

Or. en

Begründung

Diese Bestimmung ermöglicht Flexibilität für die Fälle, in denen Mitgliedstaaten bereits über Systeme verfügen (die durch ein europäisches System für die Cybersicherheit ersetzt werden müssen, sobald sie ablaufen), die mehr Cybersicherheit bieten als das von ENISA ausgearbeitete mögliche System.

Änderungsantrag 314
Antonio López-Istúriz White

Vorschlag für eine Verordnung
Artikel 47 – Überschrift

Vorschlag der Kommission

**Elemente der europäischen Systeme für die
Cybersicherheitszertifizierung**

Geänderter Text

**Elemente der europäischen Systeme für die
Cybersicherheit**

Or. en

Begründung

Die obige Änderung ist erforderlich, um zu gewährleisten, dass Aktualisierungen nicht automatisch Neubewertungs- oder Notifizierungsverfahren auslösen. Von Einrichtungen zu

verlangen, sich jedes Mal, wenn eine Änderung erfolgt – selbst bei Änderungen, die die Sicherheit erhöhen oder die nur die Benutzerfreundlichkeit oder Leistung betreffen –, erneut einer Konformitätsbewertung zu unterziehen, würde die Attraktivität und den Erfolg des vorgeschlagenen EU-Rahmens in hohem Maße einschränken (und könnte sogar kontraproduktive Fehlanreize zur Nichtdurchführung zeitnaher Updates in Reaktion auf festgestellte Schwachstellen schaffen).

Änderungsantrag 315
Antanas Guoga

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Einleitung

Vorschlag der Kommission

1. ***Ein europäisches System*** für die Cybersicherheitszertifizierung ***muss folgende Elemente enthalten:***

Geänderter Text

1. ***Folgende Elemente sind bei der Ausarbeitung eines europäischen Systems*** für die Cybersicherheitszertifizierung ***zu berücksichtigen:***

Or. en

Änderungsantrag 316
Dita Charanzová

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Einleitung

Vorschlag der Kommission

1. Ein europäisches System für die Cybersicherheitszertifizierung muss ***folgende*** Elemente enthalten:

Geänderter Text

1. Ein europäisches System für die Cybersicherheitszertifizierung ***muss eines oder mehrere der folgenden*** Elemente enthalten:

Or. en

Änderungsantrag 317
Roberta Metsola, Lara Comi, Eva Maydell, Carlos Coelho

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Einleitung

Vorschlag der Kommission

1. Ein europäisches System für die Cybersicherheitszertifizierung muss folgende Elemente enthalten:

Geänderter Text

1. Ein europäisches System für die Cybersicherheitszertifizierung muss **mindestens** folgende Elemente enthalten:

Or. en

Änderungsantrag 318
Antonio López-Istúriz White

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Einleitung

Vorschlag der Kommission

1. Ein europäisches System für **die Cybersicherheitszertifizierung** muss folgende Elemente enthalten:

Geänderter Text

1. Ein europäisches System für Cybersicherheit muss folgende Elemente enthalten:

Or. en

Änderungsantrag 319
Dita Charanzová

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe a

Vorschlag der Kommission

(a) Gegenstand und Umfang **der** Zertifizierung, darunter auch Art oder Kategorie der erfassten IKT-Produkte und -Dienste;

Geänderter Text

(a) Gegenstand und Umfang **des Systems für die** Zertifizierung, darunter auch Art oder Kategorie der erfassten IKT-Produkte, -Dienste **und Prozesse, da eine solche Zertifizierung für einen oder mehrere Sektor(en) bestimmt ist oder sektorübergreifend angewandt werden kann;**

Or. en

Änderungsantrag 320
Roberta Metsola, Lara Comi, Pascal Arimont, Carlos Coelho

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe a

Vorschlag der Kommission

(a) Gegenstand und Umfang der Zertifizierung, darunter auch Art oder Kategorie der erfassten **IKT-Produkte** und -Dienste;

Geänderter Text

(a) Gegenstand und Umfang der Zertifizierung, darunter auch Art oder Kategorie der erfassten **IKT-Hardware und Software-Produkte** und -Dienste;

Or. en

Änderungsantrag 321
Dita Charanzová

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe b

Vorschlag der Kommission

(b) detaillierte Spezifikation der Cybersicherheitsanforderungen, auf deren Einhaltung die jeweiligen IKT-Produkte und -Dienste geprüft werden, **z. B.** durch die Bezugnahme auf **europäische oder** internationale Normen oder technische Spezifikationen;

Geänderter Text

(b) detaillierte Spezifikation der Cybersicherheitsanforderungen, auf deren Einhaltung die jeweiligen IKT-Produkte und -Dienste geprüft werden durch die Bezugnahme auf internationale, **europäische oder nationale** Normen oder technische Spezifikationen, **die im Bewertungs- und Zertifizierungsprozess befolgt werden;**

Or. en

Änderungsantrag 322
Roberta Metsola, Lara Comi, Pascal Arimont, Carlos Coelho

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe b

Vorschlag der Kommission

(b) detaillierte Spezifikation der Cybersicherheitsanforderungen, auf deren Einhaltung die jeweiligen **IKT-Produkte** und -Dienste geprüft werden, z. B. durch

Geänderter Text

(b) detaillierte Spezifikation der Cybersicherheitsanforderungen, auf deren Einhaltung die jeweiligen **IKT-Hardware- und Software-Produkte** und -Dienste

die Bezugnahme auf europäische oder internationale Normen oder technische Spezifikationen;

geprüft werden, z. B. durch die Bezugnahme auf europäische oder internationale Normen oder technische Spezifikationen;

Or. en

Änderungsantrag 323

Anneleen Van Bossuyt, Daniel Dalton

Vorschlag für eine Verordnung

Artikel 47 – Absatz 1 – Buchstabe b

Vorschlag der Kommission

(b) detaillierte Spezifikation der Cybersicherheitsanforderungen, auf deren Einhaltung die jeweiligen IKT-Produkte und -Dienste geprüft werden, z. B. durch die Bezugnahme auf **europäische oder** internationale Normen oder technische Spezifikationen;

Geänderter Text

(b) detaillierte Spezifikation der Cybersicherheitsanforderungen, auf deren Einhaltung die jeweiligen IKT-Produkte und -Dienste geprüft werden, z. B. durch die Bezugnahme auf internationale **oder europäische** Normen oder technische Spezifikationen;

Or. en

Änderungsantrag 324

Antonio López-Istúriz White

Vorschlag für eine Verordnung

Artikel 47 – Absatz 1 – Buchstabe b

Vorschlag der Kommission

(b) detaillierte Spezifikation der Cybersicherheitsanforderungen, auf deren Einhaltung die jeweiligen IKT-Produkte und -Dienste geprüft werden, **z. B. durch die** Bezugnahme auf **europäische oder** internationale Normen oder technische Spezifikationen;

Geänderter Text

(b) detaillierte Spezifikation der Cybersicherheitsanforderungen, auf deren Einhaltung die jeweiligen IKT-Produkte und -Dienste geprüft werden, **mit besonderer** Bezugnahme auf internationale Normen oder technische Spezifikationen;

Or. en

Änderungsantrag 325
Dita Charanzová

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe b a (neu)

Vorschlag der Kommission

Geänderter Text

(ba) eine detaillierte Angabe, ob eine bewilligte Zertifizierung nur für ein einzelnes Produkt oder auf eine Produktpalette gilt [verschiedene Versionen/Modelle derselben Grundstruktur eines Produkts];

Or. en

Änderungsantrag 326
Antanas Guoga

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe b a (neu)

Vorschlag der Kommission

Geänderter Text

(ba) Bedeutung der Förderung von Sicherheit als Designkriterium;

Or. en

Änderungsantrag 327
Roberta Metsola, Eva Maydell, Lara Comi, Carlos Coelho

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe c

Vorschlag der Kommission

Geänderter Text

(c) gegebenenfalls eine oder mehrere Vertrauenswürdigkeitsstufen;

(c) gegebenenfalls eine oder mehrere **risikobasierte** Vertrauenswürdigkeitsstufen;

Or. en

Änderungsantrag 328
Andreas Schwab, Philippe Juvin

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe c

Vorschlag der Kommission

(c) gegebenenfalls eine oder mehrere
Vertrauenswürdigkeitsstufen;

Geänderter Text

(c) gegebenenfalls eine oder mehrere
Sicherheitsanforderungen;

Or. en

Änderungsantrag 329
Roberta Metsola, Eva Maydell, Lara Comi, Jiří Pospíšil

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe c a (neu)

Vorschlag der Kommission

Geänderter Text

*(ca) das anzuwendende
Konformitätsbewertungsverfahren
und/oder die Konformitäts-
Eigenerklärung*

Or. en

Änderungsantrag 330
Roberta Metsola, Eva Maydell, Lara Comi, Carlos Coelho

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe c b (neu)

Vorschlag der Kommission

Geänderter Text

*(cb) Zertifizierungsanforderungen, die
derart festgelegt werden, dass die
Zertifizierung in die vom Hersteller
während der Gestaltung, Entwicklung
und des Lebenszyklus des IKT-Produkts
oder -Dienstes befolgten, systematischen
Cybersicherheitsprozesse integriert
werden oder auf diesen basieren kann.*

Änderungsantrag 331
Antonio López-Istúriz White

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe e

Vorschlag der Kommission

(e) für die Zertifizierung *erforderliche* Informationen, die ein Antragsteller der Konformitätsbewertungsstelle vorzulegen hat;

Geänderter Text

(e) **im Zusammenhang mit der Option für eine Zertifizierung durch Dritte nach Artikel 47a Absatz 2 Buchstabe b die** für die Zertifizierung *erforderlichen* Informationen, die ein Antragsteller der Konformitätsbewertungsstelle vorzulegen hat;

Or. en

Änderungsantrag 332
Dita Charanzová

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe f

Vorschlag der Kommission

(f) **Bedingungen für die Verwendung von Siegeln oder Kennzeichen, sofern das System solche vorsieht;**

Geänderter Text

entfällt

Or. en

Änderungsantrag 333
Roberta Metsola, Lara Comi, Pascal Arimont, Carlos Coelho

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe f

Vorschlag der Kommission

(f) Bedingungen für die Verwendung

Geänderter Text

(f) Bedingungen für die Verwendung

von Siegeln oder Kennzeichen, sofern das System solche vorsieht;

von Siegeln oder Kennzeichen, sofern das System solche vorsieht, **wobei ein solches EU-Cybersicherheits-Konformitätskennzeichen bedeutet, dass das IKT-Produkt oder der IKT-Dienst den Kriterien eines europäischen Systems für Cybersicherheitszertifizierung entspricht;**

Or. en

Begründung

Wir müssen sicherstellen, dass wir Bürgern sachliche Informationen geben, auf deren Grundlage sie informierte Entscheidungen treffen können. Bürger sollten nicht dazu verleitet werden, zu glauben, dass ein Produkt frei von Risiken ist, da dies technisch nicht möglich ist und zu einer negativen Gegenreaktion gegenüber der EU führen könnte. Aus dem Kennzeichen auf dem Produkt oder den Dienst sollte klar hervorgehen, dass das Produkt oder der Dienst einem europäischen System für die Cybersicherheitszertifizierung entspricht und welcher risikobasierten Vertrauenswürdigkeitsstufe es/er entspricht.

Änderungsantrag 334

Antonio López-Istúriz White

Vorschlag für eine Verordnung

Artikel 47 – Absatz 1 – Buchstabe g

Vorschlag der Kommission

Geänderter Text

(g) Vorschriften für die Überwachung der Einhaltung der mit dem Zertifikat verbundenen Anforderungen, sofern das System eine Aufsicht vorsieht, einschließlich der Mechanismen für den Nachweis der fortgesetzten Einhaltung der festgelegten Cybersicherheitsanforderungen;

entfällt

Or. en

Änderungsantrag 335

Andreas Schwab

Vorschlag für eine Verordnung

Artikel 47 – Absatz 1 – Buchstabe g

Vorschlag der Kommission

(g) Vorschriften für die Überwachung der Einhaltung der mit dem Zertifikat verbundenen Anforderungen, sofern das System eine Aufsicht vorsieht, einschließlich der Mechanismen für den Nachweis der fortgesetzten Einhaltung der festgelegten Cybersicherheitsanforderungen;

Geänderter Text

(g) Vorschriften für die Überwachung der Einhaltung der mit dem Zertifikat verbundenen Anforderungen, sofern das System eine Aufsicht vorsieht, einschließlich der Mechanismen für den Nachweis der fortgesetzten Einhaltung der festgelegten Cybersicherheitsanforderungen, ***wo dies relevant und möglich ist, auch durch obligatorische Updates, Upgrades oder Patches für die betreffenden IKT-Produkte oder -Dienste.; Für alle IKT-Produkte und -Dienste mit mittleren oder hohen Sicherheitsanforderungen sollte eine regelmäßige Überwachung obligatorisch sein;***

Or. en

Änderungsantrag 336

Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung

Artikel 47 – Absatz 1 – Buchstabe g

Vorschlag der Kommission

(g) Vorschriften für die Überwachung der Einhaltung der mit dem Zertifikat verbundenen Anforderungen, sofern das System eine Aufsicht vorsieht, einschließlich der Mechanismen für den Nachweis der fortgesetzten Einhaltung der festgelegten Cybersicherheitsanforderungen;

Geänderter Text

(g) Vorschriften für die Überwachung der Einhaltung der mit dem Zertifikat verbundenen Anforderungen, sofern das System eine Aufsicht vorsieht, ***gegebenenfalls*** einschließlich der Mechanismen für den Nachweis der fortgesetzten Einhaltung der festgelegten Cybersicherheitsanforderungen;

Or. en

Änderungsantrag 337

Antonio López-Istúriz White

Vorschlag für eine Verordnung

Artikel 47 – Absatz 1 – Buchstabe h

Vorschlag der Kommission

Geänderter Text

(h) Bedingungen für die Gewährung, Aufrechterhaltung, Fortführung, Ausweitung und Verringerung des Zertifizierungsumfangs;

entfällt

Or. en

Änderungsantrag 338 Philippe Juvin

Vorschlag für eine Verordnung Artikel 47 – Absatz 1 – Buchstabe h

Vorschlag der Kommission

Geänderter Text

(h) Bedingungen für die Gewährung, Aufrechterhaltung, Fortführung, Ausweitung und Verringerung des Zertifizierungsumfangs;

(h) Bedingungen für die Gewährung, Aufrechterhaltung, Fortführung, **Erneuerung**, Ausweitung und Verringerung des Zertifizierungsumfangs;

Or. fr

Änderungsantrag 339 Lucy Anderson, Marc Tarabella, Christel Schaldemose, Liisa Jaakonsaari

Vorschlag für eine Verordnung Artikel 47 – Absatz 1 – Buchstabe h a (neu)

Vorschlag der Kommission

Geänderter Text

(ha) Das System für die Zertifizierung muss die Bedingungen für eine erneute Zertifizierung oder Bewertung eines Produkts oder Dienstes festlegen. Dies ist insbesondere für Softwaredienste wichtig, die kontinuierliche Sicherheits- und Updatefunktionen verarbeiten, wie z. B. Patches, bei denen eine schnelle Bewertung oder erneute Zertifizierung erforderlich ist, um nachteilige Auswirkungen auf die gesamte Sicherheit

*dieses Produkts oder Dienstes
abzuwenden.*

Or. en

Änderungsantrag 340

Arndt Kohn, Sergio Gutiérrez Prieto, Pina Picierno, Christel Schaldemose

Vorschlag für eine Verordnung

Artikel 47 – Absatz 1 – Buchstabe h a (neu)

Vorschlag der Kommission

Geänderter Text

(ha) Die spezifischen Fälle für eine erneute Zertifizierung eines IKT-Produkts oder -Dienstes werden im entsprechenden System für die Zertifizierung festgelegt. Sicherheits- und Feature-Updates im Zusammenhang mit jeglichen Sicherheitsmaßnahmen müssen einen Bewertungs- und nötigenfalls auch einen erneuten Zertifizierungsprozess durchlaufen;

Or. en

Änderungsantrag 341

Antonio López-Istúriz White

Vorschlag für eine Verordnung

Artikel 47 – Absatz 1 – Buchstabe i

Vorschlag der Kommission

Geänderter Text

(i) Vorschriften, die greifen, wenn die zertifizierten IKT-Produkte und -Dienste den Zertifizierungsanforderungen nicht genügen; *entfällt*

Or. en

Änderungsantrag 342

Roberta Metsola, Eva Maydell, Lara Comi, Carlos Coelho

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe i

Vorschlag der Kommission

(i) Vorschriften, die greifen, wenn die zertifizierten **IKT-Produkte** und -Dienste den Zertifizierungsanforderungen nicht genügen;

Geänderter Text

(i) Vorschriften, die greifen, wenn die zertifizierten **IKT-Hardware und Software-Produkte** und -Dienste den Zertifizierungsanforderungen nicht genügen, **einschließlich allgemeiner Informationen zu den Sanktionen gemäß Artikel 54**;

Or. en

Änderungsantrag 343
Roberta Metsola, Lara Comi, Pascal Arimont, Carlos Coelho

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe j

Vorschlag der Kommission

(j) Vorschriften für die Meldung und Behandlung bislang nicht erkannter Cybersicherheitsschwachstellen von **IKT-Produkten** und -Diensten;

Geänderter Text

(j) **die Anforderung, dass ein Händler oder Dienstleister eines IKT-Hardware oder Softwareprodukts über Verfahren und Vorschriften verfügt** für die Meldung und Behandlung bislang nicht erkannter Cybersicherheitsschwachstellen von **IKT-Hardware- und Software-Produkten** und -Diensten;

Or. en

Begründung

Dies beinhaltet eine umfassende Kommunikationskette zwischen Kunden, Verkäufern und Herstellern, damit der Endnutzer in der Lage ist, dem Verkäufer oder dem Hersteller nicht erkannte Cybersicherheitsschwachstellen mitzuteilen, damit zu deren Behebung Patches oder Fehlerbehebungen herausgegeben werden können.

Änderungsantrag 344
Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe j

Vorschlag der Kommission

(j) Vorschriften **für** die Meldung **und Behandlung bislang** nicht **erkannter** Cybersicherheitsschwachstellen von IKT-Produkten und -Diensten;

Geänderter Text

(j) Vorschriften, **die** die **zügige** Meldung nicht **allgemein bekannter** Cybersicherheitsschwachstellen von IKT-Produkten und -Diensten **durch die entsprechenden Behörden an betreffende Zulieferer und Hersteller erforderlich machen, indem sie einen koordinierten Prozess zur Offenlegung von Schwachstellen befolgen.**

Or. en

Begründung

Diese Aufgabe muss im Einklang mit den in den internationalen Normen ISO/IEC 29147:2014 und ISO/IEC 30111 festgelegten Leitlinien und Empfehlungen ausgeführt werden.

Änderungsantrag 345
Dita Charanzová

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe j

Vorschlag der Kommission

(j) Vorschriften **für** die Meldung **und Behandlung bislang** nicht **erkannter** Cybersicherheitsschwachstellen von IKT-Produkten und -Diensten;

Geänderter Text

(j) Vorschriften, **die** die **zügige** Meldung nicht **allgemein bekannter** Cybersicherheitsschwachstellen von IKT-Produkten und -Diensten **durch die entsprechenden Behörden an betreffende Zulieferer und Hersteller erforderlich machen, indem sie einen koordinierten Prozess zur Offenlegung von Schwachstellen befolgen;**

Or. en

Änderungsantrag 346
Jiří Pospíšil

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe j

Vorschlag der Kommission

(j) Vorschriften für die Meldung und Behandlung bislang nicht erkannter Cybersicherheitsschwachstellen von IKT-Produkten und -Diensten;

Geänderter Text

(j) Vorschriften für die Meldung und Behandlung bislang nicht erkannter Cybersicherheitsschwachstellen **und -mängel** von IKT-Produkten und -Diensten;

Or. cs

Änderungsantrag 347
Antonio López-Istúriz White

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe j

Vorschlag der Kommission

(j) Vorschriften für die **Meldung und** Behandlung bislang nicht erkannter Cybersicherheitsschwachstellen von IKT-Produkten und -Diensten;

Geänderter Text

(j) Vorschriften für die Behandlung bislang nicht erkannter Cybersicherheitsschwachstellen von IKT-Produkten und -Diensten;

Or. en

Änderungsantrag 348
Antonio López-Istúriz White

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe k

Vorschlag der Kommission

(k) Vorschriften für die Konformitätsbewertungsstellen über die Aufbewahrung von Aufzeichnungen;

Geänderter Text

(k) **im Zusammenhang mit der Option für eine Zertifizierung durch Dritte nach Artikel 47a Absatz 2 Buchstabe b** Vorschriften für die Konformitätsbewertungsstellen über die Aufbewahrung von Aufzeichnungen;

Or. en

Änderungsantrag 349
Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe l

Vorschlag der Kommission

(l) Angabe nationaler Systeme für die Cybersicherheitszertifizierung für dieselbe Art oder Kategorie von IKT-Produkten **und** -Diensten;

Geänderter Text

(l) Angabe nationaler **oder internationaler** Systeme für die Cybersicherheitszertifizierung für dieselbe Art oder Kategorie von IKT-Produkten, -Diensten, **Prozessen, Sicherheitsanforderungen sowie Evaluierungskriterien und -methoden**;

Or. en

Änderungsantrag 350
Roberta Metsola, Eva Maydell, Lara Comi

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe l

Vorschlag der Kommission

(l) Angabe nationaler Systeme für die Cybersicherheitszertifizierung für dieselbe Art oder Kategorie von **IKT-Produkten und -Diensten**;

Geänderter Text

(l) Angabe nationaler Systeme **oder von der Branche angeführter Methoden** für die Cybersicherheitszertifizierung für dieselbe Art oder Kategorie von **IKT-Hardware- und Software-Produkten** und -Diensten;

Or. en

Änderungsantrag 351
Antonio López-Istúriz White

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe l

Vorschlag der Kommission

(l) Angabe nationaler Systeme für die Cybersicherheitszertifizierung für dieselbe

Geänderter Text

(l) Angabe nationaler Systeme für die Cybersicherheitszertifizierung **oder**

Art *oder Kategorie* von IKT-Produkten und -Diensten;

Selbstbewertung für dieselbe Art *von Kategorien* von IKT-Produkten und -Diensten; *und*

Or. en

Änderungsantrag 352
Philippe Juvin

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe l

Vorschlag der Kommission

(l) Angabe nationaler Systeme für die Cybersicherheitszertifizierung für dieselbe Art oder Kategorie von IKT-Produkten und -Diensten;

Geänderter Text

(l) Angabe nationaler *oder internationaler* Systeme für die Cybersicherheitszertifizierung für dieselbe Art oder Kategorie von IKT-Produkten und -Diensten;

Or. fr

Änderungsantrag 353
Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe l a (neu)

Vorschlag der Kommission

Geänderter Text

(la) Identifizierung vorhandener internationaler Systeme zur gegenseitigen Beurteilung und Zertifizierung;

Or. en

Änderungsantrag 354
Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe m a (neu)

Vorschlag der Kommission

Geänderter Text

(ma) Steuerungsmechanismen zur Aktualisierung, Änderung und Koordinierung bestimmter Zertifizierungssysteme, insbesondere detaillierte Angaben darüber, wie ein Zertifizierungssystem angesichts zusätzlicher Sicherheitsbedrohungen ab dem Zeitpunkt ihres Bekanntwerdens zu beurteilen ist.

Or. en

Änderungsantrag 355

Marietje Schaake, Matthijs van Miltenburg, Dita Charanzová

Vorschlag für eine Verordnung

Artikel 47 – Absatz 1 – Buchstabe m a (neu)

Vorschlag der Kommission

Geänderter Text

(ma) Vorschriften darüber, wie und wann Mitgliedstaaten einander zu informieren haben, wenn sie von einer nicht allgemein bekannten Schwachstelle in einem unter diesem Zertifizierungssystem zertifizierten KT-Produkt oder -Dienst Kenntnis erlangen.

Or. en

Änderungsantrag 356

Dennis de Jong

Vorschlag für eine Verordnung

Artikel 47 – Absatz 1 – Buchstabe m a (neu)

Vorschlag der Kommission

Geänderter Text

(ma) ein Mechanismus oder Werkzeuge, um untergeordnete Versionen oder Sicherheitsupdates effizient zu verwalten (z. B. im Zusammenhang mit Patches);

Begründung

Ein Mechanismus zum Beheben untergeordneter Sicherheitsupgrades während des Lebenszyklus des Zertifikats wird benötigt, um einem zeitraubenden und kostenintensiven Prozess für eine erneute Zertifizierung jedes Mal, wenn eine Behebung oder ein Update erforderlich ist, vorzubeugen. Dieser Mechanismus ist notwendig, um mit der hohen Entwicklungsgeschwindigkeit Schritt zu halten und um bekannte Sicherheitsprobleme schnell zu beheben. Dies ist außerdem bereits gängige Praxis bei anderen vorhandenen Zertifikaten.

Änderungsantrag 357
Philippe Juvin

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe m a (neu)

Vorschlag der Kommission

Geänderter Text

(ma) maximale Gültigkeitsdauer der Zertifikate;

Or. fr

Änderungsantrag 358
Anneleen Van Bossuyt, Daniel Dalton

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe m a (neu)

Vorschlag der Kommission

Geänderter Text

(ma) die Gültigkeitsdauer ausgestellter Zertifikate.

Or. en

Änderungsantrag 359
Roberta Metsola, Eva Maydell, Lara Comi

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe m a (neu)

Vorschlag der Kommission

Geänderter Text

(ma) die Gültigkeitsdauer des Zertifikats

Or. en

Änderungsantrag 360
Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe m b (neu)

Vorschlag der Kommission

Geänderter Text

*(mb) Beständigkeits- und
Belastbarkeitsprüfung für die
Vertrauenswürdigkeitsstufen „ziemlich
sicher“ und „äußerst sicher“;*

Or. en

Änderungsantrag 361
Dita Charanzová, Morten Løkkegaard

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 – Buchstabe m c (neu)

Vorschlag der Kommission

Geänderter Text

*(mc) wo erforderlich, anwendbare
Verfahren für Konformitäts-
Eigenerklärungen für die
Vertrauenswürdigkeitsstufe „funktional
sicher“;*

Or. en

Änderungsantrag 362
Lambert van Nistelrooij

Vorschlag für eine Verordnung
Artikel 47 – Absatz 1 a (neu)

Vorschlag der Kommission

Geänderter Text

1a. ein Mechanismus oder Werkzeuge, um untergeordnete Versionen oder Sicherheitsupdates effizient zu verwalten (zum Beispiel im Zusammenhang mit Patches);

Or. en

Begründung

Ein Mechanismus zum Beheben untergeordneter Sicherheitsupgrades während des Lebenszyklus des Zertifikats wird benötigt, um einem zeitraubenden und kostenintensiven Prozess für eine erneute Zertifizierung jedes Mal, wenn eine Behebung oder ein Update erforderlich ist, vorzubeugen. Dieser Mechanismus ist notwendig, um mit der hohen Entwicklungsgeschwindigkeit Schritt zu halten und um bekannte Sicherheitsprobleme schnell zu beheben. Dies ist außerdem bereits gängige Praxis bei anderen vorhandenen Zertifikaten.

**Änderungsantrag 363
Antonio López-Istúriz White**

**Vorschlag für eine Verordnung
Artikel 47 – Absatz 2**

Vorschlag der Kommission

2. Die für das System festgelegten Anforderungen dürfen in keinem Widerspruch zu geltenden rechtlichen Anforderungen stehen, **vor allem nicht zu solchen Anforderungen**, die sich aus harmonisiertem Unionsrecht ergeben.

Geänderter Text

2. Die für das System festgelegten Anforderungen dürfen in keinem Widerspruch zu geltenden rechtlichen Anforderungen stehen, die sich aus harmonisiertem Unionsrecht ergeben.

Or. en

**Änderungsantrag 364
Dita Charanzová, Morten Løkkegaard**

**Vorschlag für eine Verordnung
Artikel 47 – Absatz 3**

Vorschlag der Kommission

3. Soweit dies in einem Rechtsakt der Union so festgelegt ist, kann eine Zertifizierung auf der Grundlage eines

Geänderter Text

3. Soweit dies in einem Rechtsakt der Union so festgelegt ist, kann eine Zertifizierung auf der Grundlage eines

europäischen Systems für die Cybersicherheitszertifizierung für den Nachweis der Konformitätsvermutung mit den Anforderungen jenes Rechtsakts verwendet werden.

europäischen Systems für die Cybersicherheitszertifizierung *als ein alternatives Mittel* für den Nachweis der Konformitätsvermutung mit den Anforderungen jenes Rechtsakts verwendet werden.

Or. en

Änderungsantrag 365
Antonio López-Istúriz White

Vorschlag für eine Verordnung
Artikel 47 – Absatz 4 a (neu)

Vorschlag der Kommission

Geänderter Text

4a. In Übereinstimmung mit dieser Vorschrift aufgebaute Systeme dürfen keine Änderungsmitteilungen, Zertifizierungsänderungen oder erneute Zertifizierungen erforderlich machen, es sei denn solche Änderungen wirken sich sehr nachteilig auf die Sicherheit von IKT-Produkten und -Diensten aus. Hierzu zählen:

- (a) eine Einschränkung des Anwendungsbereichs für ein Zertifikat;**
- (b) Erweiterungen der Prioritäten im Sinne des Artikels 45;**
- (c) Softwareupdates gemäß Artikel 45(c); und**
- (d) jede andere Maßnahme, die darauf abzielt, auf bislang nicht erkannte Cybersicherheitsschwachstellen gemäß Artikel 45 Buchstabe c) zu reagieren.**

Or. en

Änderungsantrag 366
Antonio López-Istúriz White

Vorschlag für eine Verordnung

Artikel 47a

Selbst- oder Fremdbewertung

- 1. Ein europäisches Cybersicherheitssystem muss Optionen sowohl für die Selbstbewertung als auch für die Zertifizierung durch Dritte bereitstellen, wie in Absatz 2 Buchstabe a und Buchstabe b jeweils beschrieben.**
- 2. Der Hersteller oder Zulieferer von IKT-Produkten und -Diensten kann frei entscheiden, ob die Bewertung und Zertifizierung solcher Produkte und Dienste nach einem europäischen Cybersicherheitssystem durchgeführt werden soll von:**
 - (a) dem Hersteller oder Zulieferer selbst („Selbstbewertung“); oder**
 - (b) einer in Artikel 51 genannten Konformitätsbewertungsstelle („Fremdbewertung“);**

Or. en

Begründung

Diese Änderung ergänzt die obige Änderung zu Artikel 47 und stellt sicher, dass zukünftige Systeme für Cybersicherheit Optionen sowohl für die Selbstbewertung als auch für die Zertifizierung durch Dritte bereithalten. Es sollte dem Hersteller des IKT-Produkts und -Dienstes vorbehalten sein, zu entscheiden, ob die Bewertung durch Selbst- oder Fremdbewertung durchgeführt werden soll. Dies entspricht dem gegenwärtig in bestimmten Industriesektoren weit verbreiteten Verfahren.