Europäisches Parlament
2014-2019

Ausschuss für bürgerliche Freiheiten, Justiz und Inneres

2017/0225(COD)

9.2.2018

ÄNDERUNGSANTRÄGE
20 - 125

Entwurf einer Stellungnahme
Jan Philipp Albrecht
Verordnung über die „EU-Cybersicherheitsagentur“ (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnologien („Rechtsakt zur Cybersicherheit“)

Vorschlag für eine Verordnung
(COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

AM_Com_LegOpinion

Änderungsantrag 20
Cornelia Ernst

Vorschlag für eine Verordnung
Titel

Vorschlag der Kommission	*Geänderter Text*
Vorschlag für eine	Vorschlag für eine
VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES	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“)	über die ***„Europäische Agentur für Netz- und Informationssicherheit“*** (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der ***Sicherheit*** von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit“)
(Text von Bedeutung für den EWR)	(Text von Bedeutung für den EWR)

Or. en

Änderungsantrag 21
Michał Boni, Carlos Coelho, Frank Engel

Vorschlag für eine Verordnung
Erwägung 2

Vorschlag der Kommission	*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	(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.	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. ***Dieses Ziel ist das Herzstück der Reformagenda der Kommission, die auf die Schaffung eines digitalen Binnenmarkts abzielt, zumal die IKT-Netze das Rückgrat digitaler Produkte und Dienste sind, die das Potenzial haben, das Leben in jeder Hinsicht zu erleichtern und die wirtschaftliche Entwicklung Europas voranzutreiben. Damit die Zielsetzungen des digitalen Binnenmarkts umfassend verwirklicht werden, müssen die technologischen Grundsteine gelegt worden sein, auf die wichtige Bereiche wie elektronische Gesundheitsdienste (eHealth), das Internet der Dinge, künstliche Intelligenz, Quantumtechnologie, intelligente Verkehrssysteme und fortgeschrittene Fertigung aufbauen.***
	Or. en

Änderungsantrag 22
Morten Helveg Petersen, Filiz Hyusmenova, Petr Ježek, Nathalie Griesbeck, Gérard Deprez, Louis Michel, Maite Pagazaurtundúa Ruiz

Vorschlag für eine Verordnung
Erwägung 2

Vorschlag der Kommission	*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.	(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 ***und uneinheitliche Nutzung der*** 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.

Or. en

Änderungsantrag 23
Cornelia Ernst

Vorschlag für eine Verordnung
Erwägung 2

Vorschlag der Kommission	*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	(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.	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 ***IT-Sicherheit***, 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. *(Mit dieser Änderung wird der Begriff der Cybersicherheit durch den passenderen Begriff der IT-Sicherheit ersetzt. Sie betrifft den gesamten Text.)*

Or. en

Änderungsantrag 24
Jaromír Štětina, Roberta Metsola, Axel Voss

Vorschlag für eine Verordnung
Erwägung 3

Vorschlag der Kommission	*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 in der EU notwendigen Maßnahmen zu ergreifen, um die Netz- und Informationssysteme, die Telekommunikationsnetze und die	(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. ***Ferner drohen immer häufigere, böswillige Cyberangriffe durch Akteure in Drittstaaten, bei denen es sich sowohl um Zivilpersonen als auch Regierungen handeln kann, demokratische Prozesse zu stören und demokratische Gesellschaften***

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

in ganz Europa aus dem Gleichgewicht zu bringen. 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 25
Maria Grapini

Vorschlag für eine Verordnung
Erwägung 3

Vorschlag der Kommission	*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*** 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.	(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 ***Informationssicherheit gegenüber Cyberangriffen*** 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 26
Cornelia Ernst

Vorschlag für eine Verordnung
Erwägung 3

Vorschlag der Kommission	*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 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.	(3) Mit der zunehmenden Digitalisierung und Vernetzung steigen auch die Cybersicherheitsrisiken, wodurch die Gesellschaft insgesamt anfälliger für ***Bedrohungen auf IT-Ebene*** 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 ***Bedrohungen auf IT-Ebene*** zu schützen. *(Mit dieser Änderung wird der irreführende Begriff der Cyberbedrohung durch den passenderen Begriff der „Bedrohungen auf IT-Ebene“ ersetzt. Sie betrifft den gesamten Text.)*

Or. en

Änderungsantrag 27
Cornelia Ernst

Vorschlag für eine Verordnung
Erwägung 4

Vorschlag der Kommission	*Geänderter Text*
(4) ***Cyberangriffe*** nehmen zu und eine	(4) ***Angriffe auf IT-Ebene*** nehmen zu

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

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

(Mit dieser Änderung wird der Begriff des Cyberangriffs durch den passenderen Begriff des „Angriffs auf IT-Ebene“ ersetzt. Sie betrifft den gesamten Text.)

Or. en

Änderungsantrag 28
Maria Grapini

Vorschlag für eine Verordnung
Erwägung 4

Vorschlag der Kommission	*Geänderter Text*
(4) Cyberangriffe nehmen zu und eine Wirtschaft und Gesellschaft, die durch ihre	(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 – sowohl auf Unionsebene als auch auf globaler Ebene – für die Entscheidungsträger, die Branche und die Nutzer daher gleichermaßen wichtig.	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, 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 29
Michał Boni, Carlos Coelho, Frank Engel

Vorschlag für eine Verordnung
Erwägung 5

Vorschlag der Kommission	*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	(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.

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 ***ein koordiniertes Vorgehen der EU zu erreichen und*** 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. ***Neben der unionsweiten Zertifizierung gibt es verschiedene freiwillige Maßnahmen, die – je nach Produkt, Dienstleistung, Verwendung oder Standard – breite Akzeptanz am Markt finden; diese Maßnahmen sollten ebenso wie der Bottom-up-Ansatz der Branche sowie auch die Verwendung der eingebauten Sicherheit („security by design“) sowie die Nutzung von und der Beitrag zu internationalen Standards gefördert werden.***

Or. en

Änderungsantrag 30
Jaromír Štětina, Axel Voss

Vorschlag für eine Verordnung
Erwägung 5

Vorschlag der Kommission	*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.	(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 ***des Schutzes der Privatsphäre und*** der Sicherheit ***bei*** IKT-Produkten und -Diensten zur Verfügung stünden. Eine Zertifizierung, ***mit der*** über nationale Märkte und Sektoren hinaus unionsweit einheitliche Anforderungen und Bewertungskriterien für die Cybersicherheit festgelegt werden***, kann zu dieser Zielsetzung beitragen. Dessen ungeachtet sollten auch freiwillige Maßnahmen gefördert werden, die Privatunternehmen, etwa Betreiber und***

Diensteanbieter im Bereich des Internets der Dinge, umsetzen.

Or. en

Änderungsantrag 31
Maria Grapini

Vorschlag für eine Verordnung
Erwägung 5 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(5a) Die Cybersicherheit stellt ein Aspekt der ganzheitlichen Sicherheit dar, und die Zuständigkeit und Sachkenntnis bei der Bewertung der Sicherheit verbleiben bei den Mitgliedstaaten. Die Verwaltung des Raums der Freiheit, der Sicherheit und des Rechts stellt eine gemeinsame Zuständigkeit der EU und der Mitgliedstaaten dar; angesichts der Auswirkungen der Cybersicherheit auf die nationale Sicherheit handelt es sich dabei allerdings in mehrfacher Hinsicht um eine Frage der nationalen Souveränität. Aus diesem Grund sollte die Rolle der Mitgliedstaaten und auch der nationalen Zertifizierungsbehörden im Zusammenhang mit dem einheitlichen europäischen Rahmen für die Zertifizierung nicht auf Konsultation beschränkt werden. Den Mitgliedstaaten sollte auch angesichts ihres Fachwissens eine bedeutende Rolle im Rahmen der neuen Architektur der Zertifizierung von Cybersicherheit zukommen.

Or. ro

Änderungsantrag 32
Michał Boni, Carlos Coelho, Frank Engel

Vorschlag für eine Verordnung
Erwägung 7

Vorschlag der Kommission	*Geänderter Text*
(7) Europa hat bereits wichtige Maßnahmen ergriffen, um die Cybersicherheit zu gewährleisten und das Vertrauen in die digitale Technik zu stärken. Im Jahr 2013 wurde eine EU-Cybersicherheitsstrategie verabschiedet, die der Union als Orientierung für strategische Reaktionen auf Cybersicherheitsbedrohungen und -risiken dienen soll. Im Zuge ihrer Bemühungen, den Online-Schutz der Europäerinnen und Europäer zu erhöhen, verabschiedete die Union im Jahr 2016 mit der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union den ersten Rechtsakt auf dem Gebiet der Cybersicherheit (im Folgenden die „NIS-Richtlinie“). Mit der NIS-Richtlinie ***wurden*** Anforderungen an die nationalen Fähigkeiten im Bereich der Cybersicherheit sowie erstmals Mechanismen zur Stärkung der strategischen und operativen Zusammenarbeit zwischen den Mitgliedstaaten festgelegt sowie Verpflichtungen in Bezug auf die Sicherheitsmaßnahmen und die Meldung von Sicherheitsvorfällen für die Sektoren, die für die Wirtschaft und Gesellschaft lebenswichtig sind (Energie, Verkehr, Wasserwirtschaft, Bankwesen, Finanzmarktinfrastrukturen, Gesundheit, digitale Infrastrukturen) sowie für Anbieter zentraler digitaler Dienste (Suchmaschinen, Cloud-Computing-Dienste und Online-Marktplätze) eingeführt. Eine zentrale Aufgabe bei der Umsetzung dieser Richtlinie wurde dabei der ENISA zugewiesen. Darüber hinaus ist die wirksame Bekämpfung der Cyberkriminalität als ein Aspekt bei der Verfolgung des übergeordneten Ziels einer hohen Cybersicherheit ein wichtiger Schwerpunkt der Europäischen	(7) Europa hat bereits wichtige Maßnahmen ergriffen, um die Cybersicherheit zu gewährleisten und das Vertrauen in die digitale Technik zu stärken. Im Jahr 2013 wurde eine EU-Cybersicherheitsstrategie verabschiedet, die der Union als Orientierung für strategische Reaktionen auf Cybersicherheitsbedrohungen und -risiken dienen soll. Im Zuge ihrer Bemühungen, den Online-Schutz der Europäerinnen und Europäer zu erhöhen, verabschiedete die Union im Jahr 2016 mit der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union den ersten Rechtsakt auf dem Gebiet der Cybersicherheit (im Folgenden die „NIS-Richtlinie“). Mit der NIS-Richtlinie ***wird die Strategie für den digitalen Binnenmarkt umgesetzt; ferner werden mit der NIS-Richtlinie gemeinsam mit anderen Instrumenten, etwa der Richtlinie des Europäischen über den europäischen Kodex für die elektronische Kommunikation, der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG,*** Anforderungen an die nationalen Fähigkeiten im Bereich der Cybersicherheit sowie erstmals Mechanismen zur Stärkung der strategischen und operativen Zusammenarbeit zwischen den Mitgliedstaaten festgelegt sowie Verpflichtungen in Bezug auf die Sicherheitsmaßnahmen und die Meldung von Sicherheitsvorfällen für die Sektoren, die für die Wirtschaft und Gesellschaft lebenswichtig sind (Energie, Verkehr, Wasserwirtschaft, Bankwesen, Finanzmarktinfrastrukturen, Gesundheit, digitale Infrastrukturen) sowie für Anbieter zentraler digitaler Dienste (Suchmaschinen, Cloud-Computing-Dienste und Online-Marktplätze)

Sicherheitsagenda.	eingeführt. Eine zentrale Aufgabe bei der Umsetzung dieser Richtlinie wurde dabei der ENISA zugewiesen. Darüber hinaus ist die wirksame Bekämpfung der Cyberkriminalität als ein Aspekt bei der Verfolgung des übergeordneten Ziels einer hohen Cybersicherheit ein wichtiger Schwerpunkt der Europäischen Sicherheitsagenda.
	Or. en

Änderungsantrag 33
Monika Beňová

Vorschlag für eine Verordnung
Erwägung 8

Vorschlag der Kommission	*Geänderter Text*
(8) Seit der Verabschiedung der EU-Cybersicherheitsstrategie im Jahr 2013 und der letzten Überarbeitung des Mandats der Agentur hat sich der gesamtpolitische Rahmen deutlich verändert, auch in Bezug auf die größeren Unwägbarkeiten und die geringere Sicherheit im globalen Umfeld. Vor diesem Hintergrund und angesichts der neuen Unionspolitik im Bereich der Cybersicherheit muss das Mandat der ENISA im Hinblick auf ihre neue Rolle in dem veränderten Cybersicherheitsökosystem überarbeitet werden, damit sie ***die Union wirksam darin unterstützen kann, auf die*** Herausforderungen im Bereich der Cybersicherheit ***zu reagieren***, die sich aus dieser grundlegend veränderten Bedrohungslandschaft ergeben und für die, wie in der Bewertung der Agentur bestätigt, das laufende Mandat nicht ausreicht.	(8) Seit der Verabschiedung der EU-Cybersicherheitsstrategie im Jahr 2013 und der letzten Überarbeitung des Mandats der Agentur hat sich der gesamtpolitische Rahmen deutlich verändert, auch in Bezug auf die größeren Unwägbarkeiten und die geringere Sicherheit im globalen Umfeld. Vor diesem Hintergrund und angesichts der neuen Unionspolitik im Bereich der Cybersicherheit muss das Mandat der ENISA im Hinblick auf ihre neue Rolle in dem veränderten Cybersicherheitsökosystem überarbeitet werden, damit sie ***eine Führungsrolle übernimmt, wodurch die Reaktion der Union auf*** Herausforderungen im Bereich der Cybersicherheit ***nachhaltig verbessert wird***, die sich aus dieser grundlegend veränderten Bedrohungslandschaft ergeben und für die, wie in der Bewertung der Agentur bestätigt, das laufende Mandat nicht ausreicht.
	Or. en

Änderungsantrag 34
Monika Beňová

Vorschlag für eine Verordnung
Erwägung 10

Vorschlag der Kommission	*Geänderter Text*
(10) Mit dem Beschluss 2004/97/EG, Euratom, der auf der Tagung des Europäischen Rates vom 13. Dezember 2003 angenommen wurde, legten die Vertreter der Mitgliedstaaten fest, dass die ENISA ihren Sitz in Griechenland in einer von der griechischen Regierung zu bestimmenden Stadt haben soll. Der Sitzmitgliedstaat der Agentur sollte die bestmöglichen Voraussetzungen für eine reibungslose und effiziente Tätigkeit der Agentur gewährleisten. Damit die Agentur ihre Aufgaben ordnungsgemäß und effizient erfüllen, ***Personal einstellen und binden und*** die ***Effizienz*** der ***Vernetzungsmaßnahmen steigern kann, ist es unbedingt erforderlich, sie an einem geeigneten Standort anzusiedeln***, ***der unter anderem*** eine ***angemessene Verkehrsanbindung sowie Einrichtungen für die Ehepartner*** und ***Kinder des Personals*** der Agentur ***bietet. Die erforderlichen Modalitäten sollten in einem Abkommen zwischen der Agentur und dem Sitzmitgliedstaat festgelegt*** werden, das ***nach Billigung durch den Verwaltungsrat*** der ***Agentur geschlossen wird***.	(10) Mit dem Beschluss 2004/97/EG, Euratom, der auf der Tagung des Europäischen Rates vom 13. Dezember 2003 angenommen wurde, legten die Vertreter der Mitgliedstaaten fest, dass die ENISA ihren Sitz in Griechenland in einer von der griechischen Regierung zu bestimmenden Stadt haben soll. Der Sitzmitgliedstaat der Agentur sollte die bestmöglichen Voraussetzungen für eine reibungslose und effiziente Tätigkeit der Agentur gewährleisten. Damit die Agentur ihre Aufgaben ordnungsgemäß und effizient erfüllen ***kann***, ***ist es unbedingt erforderlich, dass*** die ***Agentur – nach Billigung durch den Verwaltungsrat*** der ***Agentur – ein Abkommen mit dem Sitzmitgliedstaat schließt. Dieses Abkommen sollte Bestimmungen enthalten, mit denen für eine ordnungsgemäße und effiziente Ausübung ihrer Aufgaben gesorgt wird; nach ordnungsgemäßem Verfahren und eingehender Diskussion im Verwaltungsrat der Agentur und anderen entsprechenden Interessenträger innerhalb der Agentur kann ein Antrag auf zusätzliche Unterstützung aufgenommen werden, ebenso können Pflichten in das Abkommen aufgenommen werden, denen der Sitzstaat nachkommen muss.***

Or. en

Änderungsantrag 35
Monika Beňová

Vorschlag für eine Verordnung

Erwägung 11

Vorschlag der Kommission	*Geänderter Text*
(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.	(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. ***Dem weiteren Kapazitätsaufbau der Agentur sollte die erforderliche Aufmerksamkeit gewidmet werden.***

Or. en

Begründung

Es ist äußerst wichtig, dass Mängel in der Leistungsfähigkeit der Agentur ausgeglichen werden. Angesichts der enormen Bedeutung, die der Cybersicherheit heute zukommt und die ihr auch künftig zukommen wird, ist ein Einsatz für einen weiteren Ausbau der Agentur notwendig. Dabei ist auch an die russische Einflussnahme bei den Wahlen, das zunehmende Know-how der Supermächte und der Staaten weltweit und den anstehendem digitalem Wandel in wichtigen Sektoren zu denken.

Änderungsantrag 36
Cornelia Ernst

Vorschlag für eine Verordnung
Erwägung 11 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(11a) Die Herausforderungen auf dem Gebiet der IT-Sicherheit sind im digitalen Zeitalter oft eng mit den Herausforderungen im Bereich des Datenschutzes, des Schutzes der Privatsphäre sowie des Schutzes der elektronischen Kommunikation verbunden. Damit die Agentur

angemessen auf diese Herausforderungen reagieren kann, sollte eine enge Zusammenarbeit mit den Stellen, die im Einklang mit der Verordnung (EG) Nr. 45/2001, der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/680 und Verordnung (EG) Nr. 1211/2009 eingerichtet wurden, sowie deren regelmäßige Anhörung integraler Bestandteil der Tätigkeiten der Agentur sein.

Or. en

Begründung

Damit keine Spannungen entstehen und Synergien genutzt werden, ist eine enge Zusammenarbeit mit dem Europäischen Datenschutzbeauftragten, den nationalen Datenschutzbehörden, dem Europäischen Datenschutzausschuss und dem GEREK erforderlich.

Änderungsantrag 37
Monika Beňová

Vorschlag für eine Verordnung
Erwägung 12

Vorschlag der Kommission	*Geänderter Text*
(12) Die Agentur sollte ein hohes Niveau an Sachkenntnis entwickeln und pflegen und durch ihre Unabhängigkeit, die Qualität ihrer Beratung und der von ihr verbreiteten Informationen, die Transparenz ihrer Verfahren und Arbeitsmethoden sowie die Sorgfalt, mit der sie ihre Aufgaben erfüllt, als Bezugspunkt Vertrauen in den Binnenmarkt schaffen. Die Agentur sollte die Bemühungen der Mitgliedstaaten und der Union proaktiv unterstützen und ihre Aufgaben in uneingeschränkter Zusammenarbeit mit den Organen, Einrichtungen und sonstigen Stellen der Union und den Mitgliedstaaten	(12) Die Agentur sollte ein hohes Niveau an Sachkenntnis entwickeln und pflegen und durch ihre Unabhängigkeit, die Qualität ihrer Beratung und der von ihr verbreiteten Informationen, die Transparenz ihrer Verfahren und Arbeitsmethoden sowie die Sorgfalt, mit der sie ihre Aufgaben erfüllt, als Bezugspunkt Vertrauen in den Binnenmarkt schaffen. Die Agentur sollte die Bemühungen der Mitgliedstaaten und der Union proaktiv unterstützen und ihre Aufgaben in uneingeschränkter Zusammenarbeit mit den Organen, Einrichtungen und sonstigen Stellen der Union und den Mitgliedstaaten

wahrnehmen. Außerdem sollte sich die Agentur auf die Beiträge des Privatsektors sowie auf die Zusammenarbeit mit diesem und anderen einschlägigen Interessenträgern stützen. ***Mit einer Reihe von*** Aufgaben ***sollte bei gleichzeitiger Wahrung*** der Flexibilität ***in ihrer Tätigkeit vorgegeben werden,*** wie ***die Agentur ihre Ziele erreichen soll***.

wahrnehmen. Außerdem sollte sich die Agentur auf die Beiträge des Privatsektors sowie auf die Zusammenarbeit mit diesem und anderen einschlägigen Interessenträgern stützen. ***Es sollten eine klare Agenda sowie*** Aufgaben ***und Zielsetzungen, die die Agentur wahrnehmen bzw. verwirklichen muss, eindeutig festgelegt werden, wobei*** der ***für ihre Tätigkeit erforderlichen*** Flexibilität ***gebührend Rechnung zu tragen ist. Soweit wie möglich sollten größtmögliche Transparenz und eine möglichst umfassende Verbreitung von Informationen gesichert werden.***

Or. en

Änderungsantrag 38
Michał Boni, Carlos Coelho, Frank Engel

Vorschlag für eine Verordnung
Erwägung 14

Vorschlag der Kommission	*Geänderter Text*
(14) Die Agentur hat grundsätzlich die Aufgabe, die einheitliche Umsetzung des einschlägigen Rechtsrahmens, vor allem die wirksame Umsetzung der NIS-Richtlinie, zu unterstützen, was für die Stärkung der Abwehrfähigkeit gegen Cyberangriffe unerlässlich ist. Angesichts der sich rasch weiterentwickelnden Bedrohungen für die Cybersicherheit müssen die Mitgliedstaaten beim Aufbau der Abwehrfähigkeit gegen Cyberangriffe natürlich mit einem umfassenderen und ressortübergreifenden Konzept unterstützt werden.	(14) Die Agentur hat grundsätzlich die Aufgabe, die einheitliche Umsetzung des einschlägigen Rechtsrahmens, vor allem die wirksame Umsetzung der NIS-Richtlinie, ***der Richtlinie des Europäischen über den europäischen Kodex für die elektronische Kommunikation, der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG*** zu unterstützen, was für die Stärkung der Abwehrfähigkeit gegen Cyberangriffe unerlässlich ist. Angesichts der sich rasch weiterentwickelnden Bedrohungen für die Cybersicherheit müssen die Mitgliedstaaten beim Aufbau der Abwehrfähigkeit gegen Cyberangriffe natürlich mit einem umfassenderen und ressortübergreifenden Konzept unterstützt werden.

Or. en

Änderungsantrag 39
Elissavet Vozemberg-Vrionidi

Vorschlag für eine Verordnung
Erwägung 20

Vorschlag der Kommission	*Geänderter Text*
(20) Für ihre operativen Aufgaben sollte die Agentur im Wege einer strukturierten Zusammenarbeit in räumlicher Nähe auf den bei der CERT-EU vorhandenen Sachverstand zurückgreifen. Die strukturierte Zusammenarbeit erleichtert die notwendigen Synergien und den Aufbau von Sachkenntnis bei der ENISA. Für die Festlegung der praktischen Aspekte einer solchen Kooperation sollten zwischen den beiden Organisationen die hierfür notwendigen Modalitäten festgelegt werden.	(20) Für ihre operativen Aufgaben sollte die Agentur im Wege einer strukturierten Zusammenarbeit in räumlicher Nähe auf den bei der CERT-EU vorhandenen Sachverstand zurückgreifen***, wenn massive Cybersicherheitsvorfälle und -krisen in Europa auftreten***. Die strukturierte Zusammenarbeit erleichtert die notwendigen Synergien und den Aufbau von Sachkenntnis bei der ENISA. Für die Festlegung der praktischen Aspekte einer solchen Kooperation sollten zwischen den beiden Organisationen die hierfür notwendigen Modalitäten festgelegt werden.

Or. en

Begründung

Dies sollte im Einklang mit den operativen Aufgaben der ENISA und nur in Ausnahmefällen geschehen.

Änderungsantrag 40
Maria Grapini

Vorschlag für eine Verordnung
Erwägung 21 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(21a) Die Kommission sollte beim Schutz kritischer Informationsinfrastrukturen die Einführung einer obligatorischen

Zusammenarbeit zwischen den Mitgliedstaaten vorschlagen.

Or. ro

Änderungsantrag 41
Michał Boni, Carlos Coelho, Frank Engel

Vorschlag für eine Verordnung
Erwägung 26

Vorschlag der Kommission	*Geänderter Text*
(26) Um die Herausforderungen im Bereich der Cybersicherheit besser verstehen und den Mitgliedstaaten und EU-Organen langfristige strategische Beratung anbieten zu können, muss die Agentur aktuelle und neu auftretende Risiken analysieren. Hierzu sollte die Agentur in Zusammenarbeit mit den Mitgliedstaaten und gegebenenfalls Statistikämtern und anderen Stellen einschlägige Informationen sammeln und Analysen neu entstehender Technik sowie themenspezifische Bewertungen dazu durchführen, welche gesellschaftlichen, rechtlichen, wirtschaftlichen und regulatorischen Folgen technische Innovationen auf die Netz- und Informationssicherheit, insbesondere die Cybersicherheit, haben. Die Agentur sollte die Mitgliedstaaten sowie die Organe, Einrichtungen und sonstigen Stellen der EU darüber hinaus bei der Ermittlung sich abzeichnender Trends und bei der Vermeidung von Problemen im Zusammenhang mit der Cybersicherheit unterstützen, indem sie Analysen der Bedrohungen und Sicherheitsvorfälle durchführt.	(26) Um die Herausforderungen im Bereich der Cybersicherheit besser verstehen und den Mitgliedstaaten und EU-Organen langfristige strategische Beratung anbieten zu können, muss die Agentur aktuelle und neu auftretende Risiken***, Sicherheitsvorfälle und Schwachstellen*** analysieren. Hierzu sollte die Agentur in Zusammenarbeit mit den Mitgliedstaaten und gegebenenfalls Statistikämtern und anderen Stellen einschlägige Informationen sammeln und Analysen neu entstehender Technik sowie themenspezifische Bewertungen dazu durchführen, welche gesellschaftlichen, rechtlichen, wirtschaftlichen und regulatorischen Folgen technische Innovationen auf die Netz- und Informationssicherheit, insbesondere die Cybersicherheit, haben. Die Agentur sollte die Mitgliedstaaten sowie die Organe, Einrichtungen und sonstigen Stellen der EU darüber hinaus bei der Ermittlung sich abzeichnender Trends und bei der Vermeidung von Problemen im Zusammenhang mit der Cybersicherheit unterstützen, indem sie Analysen der Bedrohungen und Sicherheitsvorfälle ***und Schwachstellen*** durchführt.

Or. en

Änderungsantrag 42
Jaromír Štětina, Roberta Metsola

Vorschlag für eine Verordnung
Erwägung 28

Vorschlag der Kommission	*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.	(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. ***Um die Abwehrbereitschaft und Abwehrfähigkeit insgesamt zu erhöhen,*** sollte die Agentur ***darüber hinaus*** einen Beitrag ***zur Förderung bewährter*** Verfahren und Lösungen ***leisten, die sich an natürliche Personen*** und Organisationen ***richten,***, indem sie verfügbare Informationen über erhebliche Sicherheitsvorfälle sammelt und analysiert und Berichte hierüber erstellt, die Unternehmen und Bürgern ***sowie den einschlägigen Behörden auf der Ebene*** der ***EU*** und ***der Mitgliedstaaten als Leitfaden dienen können***. 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***. Mit diesen Kampagnen sollten*** sicherere Verhaltensweisen der Nutzer im Internet ***gefördert***, die Nutzer für potenzielle Bedrohungen im Internet – auch für die Cyberkriminalität wie das Abgreifen von Daten (Phishing), Botnets, Finanz- und Bankenbetrug – stärker ***sensibilisiert und die Vorteile von Datenschutz*** und ***Standardauthentifizierung mit Blick auf die Verhinderung von Daten-*** und ***Identitätsdiebstahl herausgestellt werden***. Die Agentur sollte eine zentrale Rolle dabei spielen, die Sensibilisierung der Endnutzer für die Sicherheit von Geräten zu forcieren.

Änderungsantrag 43
Morten Helveg Petersen, Pavel Telička, Filiz Hyusmenova, Petr Ježek, Nathalie Griesbeck, Gérard Deprez, Louis Michel, Maite Pagazaurtundúa Ruiz

Vorschlag für eine Verordnung
Erwägung 28

Vorschlag der Kommission	*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.	(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, ***über Cybersicherheit aufzuklären,*** 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.

Or. en

Änderungsantrag 44
Jaromír Štětina, Roberta Metsola

Vorschlag für eine Verordnung
Erwägung 28 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(28a) Die Agentur sollte die Öffentlichkeit für die Risiken des Datenbetrugs und -diebstahls sensibilisieren, die die Grundrechte natürlicher Personen erheblich beeinträchtigen, die Rechtsstaatlichkeit gefährden und die Stabilität demokratischer Gesellschaften sowie der demokratischen Prozesse in den Mitgliedstaaten erschüttern könnten.

Or. en

Änderungsantrag 45
Elissavet Vozemberg-Vrionidi

Vorschlag für eine Verordnung
Erwägung 30

Vorschlag der Kommission	*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	(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.	Europäischen Agentur für Flugsicherheit (EASA) ***zur Agentur für das europäische globale Satellitennavigationssystem (GSA)*** 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.

Or. en

Begründung

Da es Probleme mit der Cybersicherheit von Galileo, insbesondere bei den Bodensegmenten, gibt, stärkt die Zusammenarbeit mit der Agentur für das europäische globale Satellitennavigationssystem die Rolle der ENISA und verbessert zugleich die Glaubwürdigkeit von Galileo.

Änderungsantrag 46
Morten Helveg Petersen, Pavel Telička, Filiz Hyusmenova, Petr Ježek, Nathalie Griesbeck, Gérard Deprez, Louis Michel, Maite Pagazaurtundúa Ruiz

Vorschlag für eine Verordnung
Erwägung 30

Vorschlag der Kommission	*Geänderter Text*
(30) Damit die Agentur ihre Ziele in vollem Umfang verwirklichen kann, sollte sie zu den einschlägigen Organen,	(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.

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 ***auf der Ebene der EU und der Mitgliedstaaten*** 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.

Or. en

Änderungsantrag 47
Michał Boni, Carlos Coelho, Frank Engel

Vorschlag für eine Verordnung
Erwägung 35

Vorschlag der Kommission	*Geänderter Text*
(35) Die Agentur sollte die Mitgliedstaaten und die Diensteanbieter dazu anspornen, ihre allgemeinen Sicherheitsstandards zu heben, damit alle	(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.	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. ***Die Agentur sollte mit Interessenträgern zusammenarbeiten, um ein unionsweites Konzept zur verantwortungsvollen Offenlegung von Schwachstellen zu erstellen, und bewährte Verfahren auf diesem Gebiet begünstigen.***
	Or. en

Änderungsantrag 48
Jaromír Štětina, Roberta Metsola

Vorschlag für eine Verordnung
Erwägung 35

Vorschlag der Kommission	*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	(35) Die Agentur sollte die Mitgliedstaaten***, Hersteller von Hardware*** und ***Software sowie*** 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 ***dafür Sorge tragen, dass die von ihnen auf den Markt gebrachten Dienste und Produkte*** den Cybersicherheitsstandards genügen. In Zusammenarbeit mit den zuständigen Behörden kann die ENISA Informationen über das Niveau der

dem Binnenmarkt angeboten werden, Anbieter und Hersteller verwarnen und sie auffordern, die Sicherheit, auch die Cybersicherheit, ihrer Produkte und Dienste zu verbessern.

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.

Or. en

Änderungsantrag 49
Jaromír Štětina, Roberta Metsola

Vorschlag für eine Verordnung
Erwägung 37

Vorschlag der Kommission	*Geänderter Text*
(37) Die ***Probleme*** der Cybersicherheit stellen ***sich weltweit***. ***Um die*** Sicherheitsstandards, einschließlich der Festlegung gemeinsamer Verhaltensnormen, ***und den Informationsaustausch zu verbessern sowie eine zügigere*** internationale Zusammenarbeit bei der ***Abwehr*** und ***einen weltweiten gemeinsamen Ansatz für Probleme der Netz-*** und ***Informationssicherheit zu fördern***, ***bedarf es einer engeren internationalen Zusammenarbeit***. In dieser Hinsicht sollte die Agentur ein stärkeres Engagement der Union und die Zusammenarbeit mit Drittländern und internationalen Organisationen unterstützen, indem sie den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union gegebenenfalls die erforderlichen Sachkenntnisse und Analysen zur Verfügung stellt.	(37) Die ***Bedrohungen im Bereich*** der Cybersicherheit stellen ***ein weltweites Problem dar***. ***Es bedarf einer engeren internationalen Zusammenarbeit, insbesondere im Bereich des Informationsaustauschs und der Ausarbeitung gemeinsamer*** Sicherheitsstandards, einschließlich der Festlegung gemeinsamer Verhaltensnormen, ***um diese Bedrohungen einzudämmen. Überdies sollte die*** internationale Zusammenarbeit bei ***Problemen*** der ***Netz-*** und ***Informationssicherheit intensiviert*** und ***darauf hingewirkt werden***, ***dass weltweit dagegen vorgegangen wird***. In dieser Hinsicht sollte die Agentur ein stärkeres Engagement der Union und die Zusammenarbeit mit Drittländern und internationalen Organisationen unterstützen, indem sie den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union gegebenenfalls die erforderlichen Sachkenntnisse und Analysen zur Verfügung stellt.

Or. en

Änderungsantrag 50
Michał Boni, Carlos Coelho, Frank Engel

Vorschlag für eine Verordnung
Erwägung 44

Vorschlag der Kommission	*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 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.	(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. ***Da den Zertifizierungsanforderungen große Bedeutung dabei zukommt, für Vertrauen in das Internet der Dinge zu sorgen, wird die Kommission insbesondere die Maßnahmen in Betracht ziehen, die der unionsweiten Harmonisierung der Sicherheitsnormen für Geräte des Internets der Dinge dienen.***

Or. en

Änderungsantrag 51
Michał Boni, Carlos Coelho, Frank Engel

Vorschlag für eine Verordnung
Erwägung 50

Vorschlag der Kommission	*Geänderter Text*
(50) Derzeit werden IKT-Produkte und -	(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.	Dienste im Hinblick auf ihre Cybersicherheit kaum zertifiziert***. 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. ***Es wird ein bedarfsorientiertes Konzept benötigt, um dafür zu sorgen, dass Dienste und Produkte geeigneten Zertifizierungssystemen unterworfen werden. Überdies bedarf es eines risikobasierten Konzepts, anhand dessen Risiken erfolgreich ermittelt und eingedämmt werden, wobei zu berücksichtigen ist, dass ein pauschales Vorgehen nicht möglich ist.***

Or. en

Änderungsantrag 52
Maria Grapini

Vorschlag für eine Verordnung
Erwägung 50

Vorschlag der Kommission	*Geänderter Text*
(50) Derzeit werden IKT-Produkte und -	(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.	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***; diese Verfahren gehen für Unternehmen mit zusätzlichen Kosten einher***. 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 53
Morten Helveg Petersen, Pavel Telička, Filiz Hyusmenova, Petr Ježek, Nathalie Griesbeck, Gérard Deprez, Louis Michel, Maite Pagazaurtundúa Ruiz

Vorschlag für eine Verordnung
Erwägung 52

Vorschlag der Kommission	*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 -	(52) Vor diesem Hintergrund gilt es, einen ***harmonisierten*** europäischen Rahmen für die Cybersicherheitszertifizierung aufzubauen, auf dessen Grundlage die Anforderungen an die zu entwickelnden europäischen Systeme zur Zertifizierung der Cybersicherheit festgelegt werden, damit

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 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**.** 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 54
Jaromír Štětina, Roberta Metsola, Axel Voss

Vorschlag für eine Verordnung
Erwägung 55

Vorschlag der Kommission	*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,	(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.	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 ***– was auch für ihren jeweiligen Lebenszyklus gilt –***, 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 ***in enger Abstimmung mit den Mitgliedstaaten und Branchenvertretern*** festgelegt werden, etwa durch Verweise auf Normen oder technische Spezifikationen. ***Die einzelnen Zertifizierungssysteme sollten so konzipiert werden, dass alle an der Entwicklung der einschlägigen IT-Produkte und -Dienste beteiligten Akteure angehalten werden, Standards, Normen und Grundsätze zu entwickeln und zu übernehmen, die für ein höchstmögliches Maß an Sicherheit während des gesamten Lebenszyklus sorgen.***

Or. en

Änderungsantrag 55
Morten Helveg Petersen, Filiz Hyusmenova, Petr Ježek, Nathalie Griesbeck, Gérard Deprez, Louis Michel, Maite Pagazaurtundúa Ruiz

Vorschlag für eine Verordnung
Erwägung 55 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(55a) Um künftigen Handelshemmnisse vorzubeugen, sollte die ENISA ein Zertifizierungssystem mit einer globalen Perspektive erstellen. Bei der Ausarbeitung der Kriterien für das Zertifizierungssystem sollte die ENISA den Dialog mit einschlägigen Partnern in der Branche suchen, um sicherzustellen, dass eine Umsetzung am Markt möglich ist.

Or. en

Änderungsantrag 56
Maria Grapini

Vorschlag für eine Verordnung
Erwägung 56 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(56a) Dieses Verfahren für die europäische Zertifizierung muss analysiert werden, damit sich die Kosten für Hersteller nicht erhöhen.

Or. ro

Änderungsantrag 57
Michał Boni, Carlos Coelho, Frank Engel

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	(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.

anderes festgelegt ist. ***Es ist davon auszugehen, dass – nach dieser Anfangsphase und in Abhängigkeit von der Umsetzung in den Mitgliedstaaten der EU sowie des Stellenwerts eines Produkts oder eines Dienstes – für künftige Technologiegenerationen stufenweise potenziell verbindliche Systeme für IKT-Produkte und -Dienste entwickelt werden, die an den politischen Zielen von morgen ausgerichtet sind.*** 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 58
Daniel Dalton

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 Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Systeme	(57) Der Rückgriff auf eine europäische Cybersicherheitszertifizierung sollte freiwillig bleiben, sofern 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

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.	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

Das System sollte auf einer freiwilligen Teilnahme und einer Zusammenarbeit mit der Branche beruhen. Es sollte nicht so gestaltet sein, dass es auf Unionsebene obligatorisch werden kann. In der NIS-Richtlinie wird festgestellt, dass die Sicherheit von Netz- und Informationssystemen über auf Freiwilligkeit beruhenden Branchenkonzepten gefördert werden sollte.

Änderungsantrag 59
Daniel Dalton

Vorschlag für eine Verordnung
Erwägung 62

Vorschlag der Kommission	*Geänderter Text*
(62) Die Agentur sollte zur Unterstützung der Cybersicherheitszertifizierung bei der kryptografischen Genehmigung von Produkten, die in Netzen für Verschlusssachen verwendet werden, auch in Kontakt mit dem Sicherheitsausschuss des Rates und den einschlägigen nationalen Gremien stehen.	***entfällt***

Or. en

Begründung

Die Verschlüsselung in den Mitgliedstaaten und die damit einhergehenden Verfahren sollten in der Zuständigkeit der Mitgliedstaaten verbleiben, zumal sie von entscheidender Bedeutung für die nationale Sicherheit sind.

Änderungsantrag 60
Monika Hohlmeier

Vorschlag für eine Verordnung
Erwägung 62

Vorschlag der Kommission	*Geänderter Text*
(62) Die Agentur sollte zur Unterstützung der Cybersicherheitszertifizierung bei der kryptografischen Genehmigung von Produkten, die in Netzen für Verschlusssachen verwendet werden, auch in Kontakt mit dem Sicherheitsausschuss des Rates und den einschlägigen nationalen Gremien stehen.	(62) Die Agentur sollte zur Unterstützung der Cybersicherheitszertifizierung bei der kryptografischen Genehmigung von Produkten, die in Netzen für Verschlusssachen ***– die nicht gemäß Artikel 3 Absatz 3 vom Anwendungsbereich dieser Verordnung ausgenommen sind –*** verwendet werden, auch in Kontakt mit dem Sicherheitsausschuss des Rates und den einschlägigen nationalen Gremien stehen.

Or. en

Änderungsantrag 61
Cornelia Ernst

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

Vorschlag der Kommission	*Geänderter Text*
(a) die Ziele, Aufgaben und organisatorischen Aspekte der ***„EU-Cybersicherheitsagentur“*** (ENISA), im Folgenden die „Agentur“ und	(a) die Ziele, Aufgaben und organisatorischen Aspekte der ***„Europäische Agentur für Netz- und Informationssicherheit“*** (ENISA), im Folgenden die „Agentur“ und

Or. en

Änderungsantrag 62
Cornelia Ernst

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

Vorschlag der Kommission	*Geänderter Text*
(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.	(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 ***Sicherheit*** 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

Rein sprachliche Änderung, um den im Kommunikationstext enthaltenen Pleonasmus zu streichen.

Änderungsantrag 63
Jaromír Štětina, Roberta Metsola

Vorschlag für eine Verordnung
Artikel 2 – Absatz 1 – Nummer 8

Vorschlag der Kommission	*Geänderter Text*
8. „Cyberbedrohung“ bezeichnet einen möglichen Umstand oder ein mögliches Ereignis, der bzw. das Netz- und Informationssysteme, deren Nutzer und betroffene Personen beeinträchtigen könnte;	8. „Cyberbedrohung“ bezeichnet einen möglichen Umstand***, eine mögliche Kapazität*** oder ein mögliches Ereignis, der bzw. das Netz- und Informationssysteme, deren Nutzer und betroffene Personen beeinträchtigen könnte;

Or. en

Begründung

Hiermit wird ein wichtiger Aspekt hinzugefügt, der insbesondere für die Bewertung von Bedrohungen von Relevanz ist.

Änderungsantrag 64
Cornelia Ernst

Vorschlag für eine Verordnung
Überschrift II

Vorschlag der Kommission	*Geänderter Text*
ENISA – die ***„EU-Cybersicherheitsagentur“***	ENISA – die ***„Europäische Agentur für Netz- und Informationssicherheit“***

Or. en

Änderungsantrag 65
Maria Grapini

Vorschlag für eine Verordnung
Artikel 3 – Absatz 1

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

Or. ro

Änderungsantrag 66
Maria Grapini

Vorschlag für eine Verordnung
Artikel 3 – Absatz 2

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

Or. ro

Änderungsantrag 67
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 ***Sicherheit der Cyberinformationen, um Cyberangriffe zu verhindern***.

Or. ro

Änderungsantrag 68
Monika Beňová

Vorschlag für eine Verordnung
Artikel 4 – Absatz 3 – Unterabsatz 1 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	Die Agentur verfolgt das Ziel, bedrohliche Schwachstellen im Netz der Union für Cybersicherheit insgesamt und in den entsprechenden Netzen der einzelnen Mitgliedstaaten zu ermitteln. Wenn die Agentur es für erforderlich erachtet, teilt sie diese Schwachstellen dem Europäischen Parlament mit.

Or. en

Änderungsantrag 69
Morten Helveg Petersen, Pavel Telička, Filiz Hyusmenova, Petr Ježek, Nathalie Griesbeck, Gérard Deprez, Louis Michel, Maite Pagazaurtundúa Ruiz

Vorschlag für eine Verordnung
Artikel 4 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
5. Die Agentur baut die Cybersicherheitskapazitäten auf Unionsebene aus, um – vor allem bei grenzüberschreitenden Sicherheitsvorfällen – die Maßnahmen zu ergänzen, die die Mitgliedstaaten zur Vermeidung von Bedrohungen oder als Reaktion darauf ergreifen.	5. Die Agentur baut die Cybersicherheitskapazitäten auf Unionsebene aus, um – vor allem bei grenzüberschreitenden Sicherheitsvorfällen – die Maßnahmen zu ergänzen ***und zu unterstützen***, die die Mitgliedstaaten zur Vermeidung von Bedrohungen oder als Reaktion darauf ergreifen.

Or. en

Änderungsantrag 70
Elissavet Vozemberg-Vrionidi

Vorschlag für eine Verordnung
Artikel 4 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
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.	6. Die Agentur fördert die Nutzung der Zertifizierung ***und der Standardisierung sowie die Ausarbeitung europäischer und internationaler Normen zu Cybersicherheit***, 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.

Or. en

Begründung

Die Agentur übernimmt eine wichtige Funktion, wenn es darum geht, europäische und internationale Normen zu Cybersicherheit auszuarbeiten.

Änderungsantrag 71
Jaromír Štětina, Roberta Metsola, Axel Voss

Vorschlag für eine Verordnung
Artikel 4 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
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.	6. Die Agentur fördert die Nutzung der Zertifizierung, auch indem sie ***zur Ausarbeitung europäischer und internationaler Normen zu Cybersicherheit und*** 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.

Or. en

Änderungsantrag 72
Cornelia Ernst

Vorschlag für eine Verordnung
Artikel 4 – Absatz 7

Vorschlag der Kommission	*Geänderter Text*
7. Die Agentur fördert ein hohes Problembewusstsein ***der Bürger und Unternehmen*** in Fragen der Cybersicherheit.	7. Die Agentur fördert ein hohes Problembewusstsein in Fragen der Cybersicherheit.

Or. en

Begründung

Es sollte nicht nur bei den Bürgern und Unternehmen für ein Problembewusstsein gesorgt werden, sondern bei allen einschlägigen Gesellschaftsakteuren, darunter auch bei den Behörden und beim Gesetzgeber. Mit dieser Änderung werden die Adressaten bewusst offengelassen.

Änderungsantrag 73
Michał Boni, Carlos Coelho, Frank Engel

Vorschlag für eine Verordnung
Artikel 5 – Absatz 1 – Nummer 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, ***der Richtlinie über den europäischen Kodex für die elektronische Kommunikation, der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG,*** 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;

Or. en

Änderungsantrag 74
Cornelia Ernst

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

Vorschlag der Kommission	*Geänderter Text*

2a. die Stellen, die gemäß der Verordnung (EU) 2016/679 eingerichtet wurden, bei der Ausarbeitung von Leitlinien zur Festlegung von für die Verarbeitung von persönlichen Daten geltenden Bedingungen und Garantien für Sicherheitszwecke unterstützt, mit dem Ziel, Schutz vor Angriffen auf Netz- und Informationssysteme im Rahmen der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/1148 und der Richtlinie 2002/58/EG zu bieten;

Or. en

Änderungsantrag 75
Cornelia Ernst

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

Vorschlag der Kommission	*Geänderter Text*
	2b. politische Strategien vorschlägt, mit denen Bedingungen und Fristen für die Beseitigung von IT-Sicherheitslücken seitens der IKT-Dienstleister festgelegt werden, damit verhindert wird, dass Nutzer gegen Computer gerichteten Angriffen ausgesetzt werden;

Or. en

Änderungsantrag 76
Cornelia Ernst

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

Vorschlag der Kommission	*Geänderter Text*
	2c. Behörden politische Strategien dafür vorschlägt, wie mit der Öffentlichkeit unbekannten Schwachstellen umzugehen ist, wobei das

Ziel verfolgt wird, die Integrität des aus verschiedenen Informationssystemen bestehenden Gesamtsystems zu erhalten;

Or. en

Änderungsantrag 77
Cornelia Ernst

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

Vorschlag der Kommission	*Geänderter Text*
	2d. politische Strategien vorschlägt und Behörden dabei berät, wie der Einsatz von proprietären IT-Lösungen vermieden oder begrenzt werden kann, um zu verhindern, dass das entsprechende Gesamtsystem Schwachstellen und insbesondere Hintertüren enthält;

Or. en

Änderungsantrag 78
Elissavet Vozemberg-Vrionidi

Vorschlag für eine Verordnung
Artikel 6 – Absatz 1 – Buchstabe a

Vorschlag der Kommission	*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;	(a) die Mitgliedstaaten bei ihren Bemühungen zur Verhütung, Erkennung und Analyse und zur Stärkung ihrer Kapazitäten für die Bewältigung von ***Cyberbedrohungen*** und ***-vorfällen***, indem sie ihnen das erforderliche Wissen und die notwendigen Sachkenntnisse zur Verfügung stellt;

Or. en

Begründung

Geeignetere Formulierung.

Änderungsantrag 79
Elissavet Vozemberg-Vrionidi

Vorschlag für eine Verordnung
Artikel 6 – Absatz 1 – Buchstabe b

Vorschlag der Kommission	*Geänderter Text*
(b) die Organe, Einrichtungen und sonstigen Stellen der Union 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 das CERT für die Organe, Agenturen und sonstigen Einrichtungen der Union (CERT-EU) angemessen unterstützt;	(b) die Organe, Einrichtungen und sonstigen Stellen der Union bei ihren Bemühungen zur Verhütung, Erkennung und Analyse und zur Stärkung ihrer Kapazitäten für die Bewältigung von ***Cyberbedrohungen*** und ***-vorfällen***, indem sie das CERT für die Organe, Agenturen und sonstigen Einrichtungen der Union (CERT-EU) angemessen unterstützt;

Or. en

Begründung

Geeignetere Formulierung.

Änderungsantrag 80
Morten Helveg Petersen, Filiz Hyusmenova, Petr Ježek, Nathalie Griesbeck, Gérard Deprez, Louis Michel, Maite Pagazaurtundúa Ruiz

Vorschlag für eine Verordnung
Artikel 6 – Absatz 1 – Buchstabe f a (neu)

Vorschlag der Kommission	*Geänderter Text*
	(fa) die nationalen Aufsichtsbehörden im Bereich des Datenschutzes und arbeitet mit ihnen gegebenenfalls zusammen.

Or. en

Änderungsantrag 81
Maria Grapini

Vorschlag für eine Verordnung
Artikel 7 – Absatz 5 – Unterabsatz 1

Vorschlag der Kommission	*Geänderter Text*
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.	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 82
Elissavet Vozemberg-Vrionidi

Vorschlag für eine Verordnung
Artikel 7 – Absatz 5 – Unterabsatz 2

Vorschlag der Kommission	*Geänderter Text*
Der Umfang der Untersuchung und das bei einer solchen Untersuchung einzuhaltende Verfahren werden zwischen den betroffenen Mitgliedstaaten und der Agentur vereinbart; etwaige laufende strafrechtliche Untersuchungen desselben	Der Umfang der Untersuchung und das bei einer solchen Untersuchung einzuhaltende Verfahren werden zwischen den betroffenen Mitgliedstaaten und der Agentur vereinbart; etwaige laufende strafrechtliche Untersuchungen desselben

Sicherheitsvorfalls bleiben hiervon unberührt. Zum Abschluss der Untersuchung erstellt die Agentur einen technischen Abschlussbericht, in den insbesondere die Informationen und Kommentare der betroffenen Mitgliedstaaten und Unternehmen einfließen und der mit den betroffenen Mitgliedstaaten abgestimmt wird. Eine Zusammenfassung des Berichts mit den Empfehlungen zur Vermeidung künftiger Sicherheitsvorfälle wird dem CSIRTs-Netz zugeleitet.	Sicherheitsvorfalls bleiben hiervon unberührt. ***Die Untersuchungen dürfen die grundlegenden Interessen der Mitgliedstaaten hinsichtlich ihrer nationalen Sicherheit nicht verletzen.*** Zum Abschluss der Untersuchung erstellt die Agentur einen technischen Abschlussbericht, in den insbesondere die Informationen und Kommentare der betroffenen Mitgliedstaaten und Unternehmen einfließen und der mit den betroffenen Mitgliedstaaten abgestimmt wird. Eine Zusammenfassung des Berichts mit den Empfehlungen zur Vermeidung künftiger Sicherheitsvorfälle wird dem CSIRTs-Netz zugeleitet.

Or. en

Begründung

Es wird hinzugefügt, dass die Untersuchungen die grundlegenden Interessen der Mitgliedstaaten hinsichtlich ihrer nationalen Sicherheit nicht verletzen dürfen.

Änderungsantrag 83
Elissavet Vozemberg-Vrionidi

Vorschlag für eine Verordnung
Artikel 8 – Absatz 1 – Buchstabe a – Nummer 1

Vorschlag der Kommission	*Geänderter Text*
(1) mögliche europäische Systeme für die Cybersicherheitszertifizierung von IKT-Produkten und -Diensten nach Artikel 44 dieser Verordnung ausarbeitet;	(1) mögliche europäische Systeme für die Cybersicherheitszertifizierung von IKT-Produkten und -Diensten ***in Zusammenarbeit mit der Branche und*** nach Artikel 44 dieser Verordnung ausarbeitet;

Or. en

Begründung

Die Zusammenarbeit ist in diesem Bereich äußerst wichtig.

Änderungsantrag 84
Jaromír Štětina, Roberta Metsola, Axel Voss

Vorschlag für eine Verordnung
Artikel 8 – Absatz 1 – Buchstabe a – Nummer 1

Vorschlag der Kommission	*Geänderter Text*
(1) mögliche europäische Systeme für die Cybersicherheitszertifizierung von IKT-Produkten und -Diensten nach Artikel 44 dieser Verordnung ausarbeitet;	(1) mögliche europäische Systeme für die Cybersicherheitszertifizierung von IKT-Produkten und -Diensten ***in Zusammenarbeit mit der Branche*** nach Artikel 44 dieser Verordnung ausarbeitet;

Or. en

Begründung

Steht in Zusammenhang mit den Änderungen an Artikel 44.

Änderungsantrag 85
Cornelia Ernst

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

Vorschlag der Kommission	*Geänderter Text*
	(ba) unterstützt die Ausarbeitung und Übernahme europäischer und internationaler Normen für die Sicherheit von IKT-Produkten und -Diensten, wobei das Ziel verfolgt wird, die absichtliche und unabsichtliche Nutzung und Verbreitung von Technologie bzw. von Teilen dieser Technologie zu verhindern, durch die die Sicherheit von IKT-Produkten und -Diensten absichtlich geschwächt wird (Hintertüren);

Or. en

Begründung

Bei einem geeigneten Zertifizierungssystem sollte die Nutzung von Hintertüren bei IKT-Produkten und -Diensten pauschal ausgeschlossen werden.

Änderungsantrag 86
Jaromír Štětina, Roberta Metsola

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 ***sowie von den Mitgliedstaaten und öffentlichen und privaten Interessenträgern*** bereitgestellten Informationen zur Cybersicherheit, ordnet diese Informationen und stellt sie über ein eigenes Portal der Öffentlichkeit zur Verfügung;

Or. en

Änderungsantrag 87
Morten Helveg Petersen, Filiz Hyusmenova, Petr Ježek, Nathalie Griesbeck, Gérard Deprez, Louis Michel, Maite Pagazaurtundúa Ruiz

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

Vorschlag der Kommission	*Geänderter Text*
(e) sensibilisiert die Öffentlichkeit für Cybersicherheitsrisiken und stellt Leitlinien für bewährte Verfahren zur Verfügung, die sich an Bürger und Organisationen wenden;	(e) sensibilisiert die Öffentlichkeit für Cybersicherheitsrisiken***, informiert über geeignete Maßnahmen zur Verhütung von Vorfällen*** und stellt Leitlinien für bewährte Verfahren zur Verfügung, die sich an Bürger und Organisationen wenden;

Or. en

Änderungsantrag 88
Jaromír Štětina, Roberta Metsola

Vorschlag für eine Verordnung

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

Vorschlag der Kommission	*Geänderter Text*
	(ea) schafft ein Netz nationaler Bildungskontaktstellen, die eine bessere Koordinierung und den Austausch bewährter Verfahren zwischen den Mitgliedstaaten unterstützen, wenn es darum geht, über Cybersicherheit aufzuklären und für das Thema zu sensibilisieren.

Or. en

Begründung

Die Schaffung eines solchen Netzes unter der Aufsicht der Agentur könnte dazu beitragen, dass die zuständigen nationalen Einrichtungen besser über die Maßnahmen informiert sind, die in anderen Mitgliedstaaten ausgearbeitet wurden. Zugleich sollte die Verbreitung bewährter Verfahren intensiviert werden, etwa die Erstellung einer Spezialausbildung für den Bereich Cybersicherheit.

Änderungsantrag 89
Jaromír Štětina, Roberta Metsola

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

Vorschlag der Kommission	*Geänderter Text*
(g) organisiert in Zusammenarbeit mit den Mitgliedstaaten sowie den Organen, Einrichtungen und sonstigen Stellen der Union regelmäßige Aufklärungskampagnen, um die Cybersicherheit und ihre Sichtbarkeit in der Union zu erhöhen.	(g) organisiert in Zusammenarbeit mit den Mitgliedstaaten sowie den Organen, Einrichtungen und sonstigen Stellen der Union ***sowie anderen einschlägigen Interessenträgern*** regelmäßige Aufklärungskampagnen, um die Cybersicherheit und ihre Sichtbarkeit in der Union zu erhöhen.

Or. en

Änderungsantrag 90
Elissavet Vozemberg-Vrionidi

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

Vorschlag der Kommission	*Geänderter Text*
(g) organisiert in Zusammenarbeit mit den Mitgliedstaaten sowie den Organen, Einrichtungen und sonstigen Stellen der Union regelmäßige Aufklärungskampagnen, um die Cybersicherheit und ihre Sichtbarkeit in der Union zu erhöhen.	(g) organisiert in Zusammenarbeit mit den Mitgliedstaaten sowie den Organen, Einrichtungen und sonstigen Stellen der Union ***sowie der Branche*** regelmäßige Aufklärungskampagnen, um die Cybersicherheit und ihre Sichtbarkeit in der Union zu erhöhen.

Or. en

Begründung

Die Zusammenarbeit ist in diesem Bereich äußerst wichtig.

Änderungsantrag 91
Elissavet Vozemberg-Vrionidi

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 aufzuklären und für das Thema zu sensibilisieren, indem ein Netz nationaler Bildungskontaktstellen geschaffen und unterhalten wird.

Or. en

Begründung

Mit einer Koordinierung und einem Austausch bewährter Verfahren zwischen den Mitgliedstaaten über ein Netz nationaler Bildungskontaktstellen kann für das Thema Cybersicherheit sensibilisiert werden.

Änderungsantrag 92
Cornelia Ernst

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

Änderungsantrag 93
Daniel Dalton

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 Informations- und Kommunikationstechnik (IKT), geschaffen und die Techniken zur Risikovermeidung genutzt werden können;	(a) berät die Agentur die Union und die Mitgliedstaaten zum Forschungsbedarf und zu den Forschungsprioritäten im Bereich der Cybersicherheit ***nur***, 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

Die ENISA hat einen klaren Aufgabenbereich, was die Cybersicherheit anbelangt. Arbeiten zu anderen Themen, etwa Datenschutz und Schutz der Privatsphäre, fallen in den Aufgabenbereich bestehender Exekutivagenturen und sollten nicht doppelt ausgeführt werden.

Änderungsantrag 94
Maria Grapini

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

Vorschlag der Kommission	*Geänderter Text*
(m) ernennt den Exekutivdirektor und verlängert gegebenenfalls dessen Amtszeit oder enthebt ihn nach Artikel 33 seines Amtes;	(m) ernennt den Exekutivdirektor ***im Rahmen einer Auswahl auf der Grundlage beruflicher Kriterien*** und verlängert gegebenenfalls dessen Amtszeit oder enthebt ihn nach Artikel 33 seines Amtes;

Or. ro

Änderungsantrag 95
Elissavet Vozemberg-Vrionidi

Vorschlag für eine Verordnung
Artikel 19 – Absatz 5

Vorschlag der Kommission	*Geänderter Text*
5. Der Exekutivdirektor beschließt, inwieweit es notwendig ist, Mitarbeiter in einem oder mehreren Mitgliedstaaten einzusetzen, damit die Agentur ihre Aufgaben effizient und wirksam wahrnehmen kann. Bevor er über die Einrichtung einer Außenstelle beschließt, holt der Exekutivdirektor die vorherige Zustimmung der Kommission, des Verwaltungsrats und des betreffenden Mitgliedstaats bzw. der betreffenden Mitgliedstaaten ein. In dem Beschluss wird der Umfang der in der Außenstelle auszuübenden Tätigkeiten so festgelegt, dass unnötige Kosten und eine	***entfällt***

Überschneidung der Verwaltungsfunktionen mit denen der Agentur vermieden werden. Soweit dies angemessen oder notwendig ist, wird mit dem/den betreffenden Mitgliedstaat(en) eine entsprechende Vereinbarung getroffen.

Or. en

Begründung

Der Aufgabenbereich der ENISA erfordert keine Präsenz in anderen Mitgliedstaaten, wie die beispielsweise die Sonderfälle Frontex und EASO erfordern. Ferner verursacht dieses Vorgehen Zusatzkosten und höhere Ausgaben.

Änderungsantrag 96
Michał Boni, Carlos Coelho, Frank Engel

Vorschlag für eine Verordnung
Artikel 20 – Absatz 1

Vorschlag der Kommission	*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 sowie Vertreter der zuständigen Behörden, die gemäß der [Richtlinie über den Europäischen Kodex für elektronische Kommunikation] notifiziert wurden, sowie Strafverfolgungsbehörden und Datenschutz-Aufsichtsbehörden.	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, ***die europäischen Normungsgremien,*** 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 97
Daniel Dalton

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

Vorschlag der Kommission	*Geänderter Text*
	5a. Bei der Ausarbeitung des möglichen Systems gemäß Artikel 44 Absatz 1 werden im Rahmen einer offiziellen Konsultation die Ständige Gruppe der Interessenträger sowie zahlreiche Branchenvertreter angehört.

Or. en

Begründung

Die Branche sollte in den Entwurf und die Ausarbeitung möglicher Systeme auf dem Wege der Konsultation einbezogen werden, damit sie ihr Fachwissen für deren effiziente Gestaltung einbringen kann.

Änderungsantrag 98
Jaromír Štětina

Vorschlag für eine Verordnung
Artikel 30 – Absatz 1

Vorschlag der Kommission	*Geänderter Text*
1. Zur Erleichterung der Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen gemäß der Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates[39] tritt die Agentur ***binnen sechs Monaten nach Aufnahme ihrer Tätigkeit*** der Interinstitutionellen Vereinbarung vom 25. Mai 1999 über die internen Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) bei und erlässt die einschlägigen Vorschriften, die für sämtliche Mitarbeiter der Agentur gelten, nach dem Muster im Anhang der genannten Vereinbarung.	1. Zur Erleichterung der Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen gemäß der Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates[39] tritt die Agentur der Interinstitutionellen Vereinbarung vom 25. Mai 1999 über die internen Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) bei und erlässt ***unverzüglich*** die einschlägigen Vorschriften, die für sämtliche Mitarbeiter der Agentur gelten, nach dem Muster im Anhang der genannten Vereinbarung.

[39] Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates vom 11. September 2013 über die Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) und zur Aufhebung der Verordnung (EG) Nr. 1073/1999 des Europäischen Parlaments und des Rates und der Verordnung (Euratom) Nr. 1074/1999 des Rates (ABl. L 248 vom 18.9.2013, S. 1).

[39] Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates vom 11. September 2013 über die Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) und zur Aufhebung der Verordnung (EG) Nr. 1073/1999 des Europäischen Parlaments und des Rates und der Verordnung (Euratom) Nr. 1074/1999 des Rates (ABl. L 248 vom 18.9.2013, S. 1).

Or. en

Änderungsantrag 99
Jaromír Štětina, Roberta Metsola

Vorschlag für eine Verordnung
Artikel 30 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
2. Der Rechnungshof ist befugt, bei allen Empfängern von Finanzhilfen sowie bei Auftragnehmern und Unterauftragnehmern, die Unionsmittel von der Agentur erhalten haben, Rechnungsprüfungen anhand von Unterlagen und ***vor Ort*** durchzuführen.	2. Der Rechnungshof ist befugt, bei allen Empfängern von Finanzhilfen sowie bei Auftragnehmern und Unterauftragnehmern, die Unionsmittel von der Agentur erhalten haben, Rechnungsprüfungen anhand von Unterlagen und ***Vorortinspektionen*** durchzuführen.

Or. en

Änderungsantrag 100
Michał Boni, Carlos Coelho, Frank Engel

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	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.	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 können*** der Kommission die Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung vorschlagen.

Or. en

Änderungsantrag 101
Jaromír Štětina, Axel Voss

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. 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 nach Artikel 53 eingesetzte Europäische Gruppe für die Cybersicherheitszertifizierung (im Folgenden die „Gruppe“) ***oder Branchenvertreter können*** der Kommission die Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung vorschlagen.

Or. en

Begründung

Zum Zwecke der Übereinstimmung mit Erwägung 53. Eine ausdrückliche Zusammenarbeit mit Interessenträgern des Privatsektors verleiht dem Verfahren zusätzliche Inklusivität.

Änderungsantrag 102
Michał Boni, Carlos Coelho, Frank Engel

Vorschlag für eine Verordnung
Artikel 44 – Absatz 2

Vorschlag der Kommission	*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.	2. Bei der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert die ENISA alle in Frage kommenden Interessenträger und arbeitet eng mit der Gruppe ***und der Ständigen Gruppe der Interessenträger*** zusammen. Die Gruppe ***und die Ständige Gruppe der 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. ***Die ENISA kann soweit erforderlich zusätzlich eine Zertifizierungsarbeitsgruppe der Interessenträger einrichten, die Mitglieder der Ständigen Gruppe der Interessenträger und andere einschlägige Interessenträger umfasst und Beratung durch Sachverständige zu Bereichen bietet, die durch ein bestimmtes mögliches System abgedeckt werden.***

Or. en

Änderungsantrag 103
Cornelia Ernst

Vorschlag für eine Verordnung
Artikel 44 – Absatz 2

Vorschlag der Kommission	*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	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 Stellen, die im Einklang mit der***

Ausarbeitung des möglichen Systems geforderte Unterstützung und fachliche Beratung und gibt nötigenfalls auch eine Stellungnahme hierzu ab.	***Verordnung (EG) Nr. 45/2001, der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/680 und der Verordnung (EG) Nr. 1211/2009 eingerichtet wurden,*** 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 104
Daniel Dalton

Vorschlag für eine Verordnung
Artikel 44 – Absatz 2

Vorschlag der Kommission	*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.	2. Bei der Ausarbeitung der möglichen Systeme nach Absatz 1 konsultiert die ENISA alle in Frage kommenden Interessenträger***, darunter Branchenvertreter, im Rahmen einer offiziellen Konsultation*** 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

Begründung

Branche und Normungsgremien sollten im Wege der Konsultation in den Entwurf und die Ausarbeitung möglicher Systeme einbezogen werden, damit sie ihr Fachwissen für deren effiziente Gestaltung einbringen kann.

Änderungsantrag 105
Monika Hohlmeier

Vorschlag für eine Verordnung
Artikel 44 – Absatz 3

Vorschlag der Kommission	*Geänderter Text*
3. Die ENISA legt der Kommission das nach Absatz 2 ausgearbeitete mögliche europäische System für die Cybersicherheitszertifizierung vor.	3. Die ENISA legt der Kommission das nach Absatz 2 ausgearbeitete mögliche europäische System für die Cybersicherheitszertifizierung ***nach der Genehmigung durch die Gruppe*** vor.

Or. en

Änderungsantrag 106
Cornelia Ernst

Vorschlag für eine Verordnung
Artikel 44 – Absatz 4

Vorschlag der Kommission	*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.	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 konsultiert gegebenenfalls den Europäischen Datenschutzausschuss, bevor sie einen solchen Beschluss fasst, damit für Kohärenz mit den gemäß der Richtlinie (EU) 2016/679 vorgenommenen Zertifizierungen gesorgt wird.***

Or. en

Änderungsantrag 107
Daniel Dalton

Vorschlag für eine Verordnung
Artikel 45 – Absatz 1 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
Für die Cybersicherheitszertifizierung wird ein europäisches System konzipiert, das – ***soweit zutreffend*** – den folgenden Sicherheitszielen Rechnung trägt:	Für die Cybersicherheitszertifizierung wird ein europäisches System konzipiert, das – ***im Verhältnis zu den Risiken im allgemeinen Betriebsumfeld der Nutzer und sofern die Nutzer angemessene Maßnahmen treffen*** – den folgenden Sicherheitszielen Rechnung trägt:

Or. en

Begründung

Die Sicherheitsziele sollten einen gewissen Spielraum bieten, damit der Verwendung von IKT-Geräten und -Diensten in verschiedenen Situationen sowie auch der Rolle, die die Nutzer mit Blick auf die Verwirklichung von Sicherheitszielen übernehmen müssen, Rechnung getragen werden kann.

Änderungsantrag 108
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 eine oder mehrere der Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ bzw. „hoch“ angeben***, darunter auch für die verschiedenen individuellen Anwendungsfälle***.

Or. en

Begründung

Damit wird den Anbietern Spielraum geboten, für die verschiedenen Anwendungsfälle, die für IKT-Produkte und -Dienste infrage kommen, verschiedene Vertrauenswürdigkeitsstufen anzugeben.

Änderungsantrag 109
Michał Boni, Carlos Coelho, Frank Engel

Vorschlag für eine Verordnung
Artikel 46 – Absatz 2 – Einleitung

Vorschlag der Kommission	*Geänderter Text*
2. Die Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ bzw. „hoch“ ***erfüllen jeweils folgende Kriterien:***	2. Die Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ bzw. „hoch“ ***beziehen sich auf ein im Rahmen einer europäischen Cybersicherheitszertifizierung ausgestelltes Zertifikat, das ein entsprechendes Maß an Vertrauen in die beanspruchten oder geltend gemachten 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 Vertrauenswürdigkeitsstufen werden fallweise festgelegt.***

Or. en

Änderungsantrag 110
Michał Boni, Carlos Coelho, Frank Engel

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	***entfällt***

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 111
Daniel Dalton

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.	(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***, vorausgesetzt, dass die Nutzer angemessene Maßnahmen treffen***.

Or. en

Begründung

Es sollte nicht das Risiko eingegangen werden, dass Verbraucher zu sehr auf Zertifikate vertrauen. Ebenso wenig sollte die Branche dazu gedrängt werden, Zeit und Ressourcen für eine hohe Vertrauenswürdigkeitsstufe zu investieren, da damit die Markteinführung verzögert und die Nachfrageorientierung verringert wird und gleichzeitig die Vorsichtsmaßnahmen der Nutzer außer Acht gelassen werden.

Änderungsantrag 112
Michał Boni, Carlos Coelho, Frank Engel

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 113
Daniel Dalton

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	(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.	Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen – deren Zweck in der Minderung der Gefahr von Cybersicherheitsvorfällen besteht – gekennzeichnet ist***, vorausgesetzt, dass die Nutzer angemessene Maßnahmen treffen***.

Or. en

Begründung

Siehe oben.

Änderungsantrag 114
Michał Boni, Carlos Coelho, Frank Engel

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 115
Daniel Dalton

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.	(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***, vorausgesetzt, dass die Nutzer angemessene Maßnahmen treffen***.

Or. en

Begründung

Siehe oben.

Änderungsantrag 116
Michał Boni, Carlos Coelho, Frank Engel

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

Vorschlag der Kommission	*Geänderter Text*
	(aa) Konformitätsbewertungs- und Prüfstellen;

Or. en

Änderungsantrag 117

Michał Boni, Carlos Coelho, Frank Engel

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

Vorschlag der Kommission	*Geänderter Text*
(l) Angabe nationaler Systeme für die Cybersicherheitszertifizierung für dieselbe Art oder Kategorie von IKT-Produkten und -Diensten;	(l) Angabe nationaler Systeme für die Cybersicherheitszertifizierung ***im Sinne von Artikel 49*** für dieselbe Art oder Kategorie von IKT-Produkten und -Diensten;

Or. en

Änderungsantrag 118
Daniel Dalton

Vorschlag für eine Verordnung
Artikel 48 – Absatz 2

Vorschlag der Kommission	*Geänderter Text*
2. Die Zertifizierung ist freiwillig***, sofern nicht anderweitig im Unionsrecht festgelegt***.	2. Die Zertifizierung ist freiwillig.

Or. en

Begründung

Das System sollte auf einer freiwilligen Teilnahme und einer Zusammenarbeit mit der Branche beruhen. Es sollte nicht so gestaltet sein, dass es auf Unionsebene obligatorisch werden kann. In der NIS-Richtlinie wird festgestellt, dass die Sicherheit von Netz- und Informationssystemen über auf Freiwilligkeit beruhende Branchenkonzepte gefördert werden sollte.

Änderungsantrag 119
Daniel Dalton

Vorschlag für eine Verordnung
Artikel 48 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*

6. Zertifikate werden für eine Höchstdauer ***von drei Jahren*** erteilt und können unter denselben Bedingungen verlängert werden, sofern die einschlägigen Voraussetzungen weiterhin erfüllt werden.	6. Zertifikate werden für eine ***im Zertifizierungssystem festgesetzte*** Höchstdauer erteilt und können unter denselben Bedingungen verlängert werden, sofern die einschlägigen Voraussetzungen weiterhin erfüllt werden.

Or. en

Begründung

Zertifizierungen können zwischen 12 und 18 Monaten in Anspruch nehmen und bilden die Sicherheit ab, die für ein bestimmtes Produkt zu einem bestimmten Zeitpunkt gilt.

Änderungsantrag 120
Monika Hohlmeier

Vorschlag für eine Verordnung
Artikel 48 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
6. Zertifikate werden für ***eine Höchstdauer von drei Jahren*** erteilt und können unter denselben Bedingungen verlängert werden, sofern die einschlägigen Voraussetzungen weiterhin erfüllt werden.	6. Zertifikate werden für ***die im entsprechenden Zertifizierungssystem festgesetzte Dauer*** erteilt und können unter denselben Bedingungen verlängert werden, sofern die einschlägigen Voraussetzungen weiterhin erfüllt werden.

Or. en

Änderungsantrag 121
Michał Boni, Carlos Coelho, Jaromír Štětina, Frank Engel

Vorschlag für eine Verordnung
Artikel 48 – Absatz 6

Vorschlag der Kommission	*Geänderter Text*
6. Zertifikate werden für eine Höchstdauer ***von drei Jahren*** erteilt und können unter denselben Bedingungen verlängert werden, sofern die einschlägigen Voraussetzungen weiterhin erfüllt werden.	6. Zertifikate werden für eine ***für jedes Zertifizierungssystem fallweise festgesetzte*** Höchstdauer erteilt und können unter denselben Bedingungen verlängert werden, sofern die einschlägigen

Voraussetzungen weiterhin erfüllt werden.

Or. en

Änderungsantrag 122
Jan Philipp Albrecht

Vorschlag für eine Verordnung
Artikel 48 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	Artikel 48a
	Grundanforderungen im Bereich der IT-Sicherheit
	1. Die Agentur schlägt der Kommission bis [zwei Jahre nach Inkrafttreten der Verordnung] klare obligatorische Grundanforderungen im Bereich der IT-Sicherheit für alle IT-Geräte vor, die in der Union verkauft oder aus der Union ausgeführt werden, darunter folgende Anforderungen:
	(a) Der Anbieter legt eine schriftliche Bescheinigung darüber vor, dass das Gerät keine Hardware, Software oder Firmware mit bekannten Sicherheitslücken enthält.
	(b) Das Gerät ist mit Software bzw. Firmware ausgestattet, die vom Anbieter bereitgestellte ordnungsgemäß authentifizierte und aus vertrauenswürdiger Quelle stammende Aktualisierungen ermöglicht.
	(c) Die dokumentierten Fernzugriffsmöglichkeiten auf das Gerät werden spätestens bei der Installation gegen einen unbefugten Zugriff gesichert. Es gibt kein hartcodiertes Standardkennwort für alle Geräte; es besteht die dokumentierte Möglichkeit, Aktualisierungen vorzunehmen, wobei eindeutig auf die Verantwortung in dem Fall hingewiesen wird, dass der Nutzer

das Gerät nicht aktualisiert.

(d) Der Anbieter von Geräten, Software oder Firmware, die mit dem Internet verbunden sind, ist verpflichtet, den zuständigen Behörden alle bekannten Sicherheitslücken zu melden.

(e) Der Anbieter von Geräten, Software oder Firmware, die mit dem Internet verbunden sind, ist verpflichtet, eine Reparatur oder einen Ersatz anzubieten, wenn eine neue Sicherheitslücke entdeckt wird.

(f) Der Anbieter von Geräten, Software oder Firmware, die mit dem Internet verbunden sind, ist verpflichtet, darüber zu informieren, wie die Geräte Aktualisierungen erhalten und wann die Sicherheitsunterstützung planmäßig ausläuft, und wie förmlich mitgeteilt wird, dass eine solche Sicherheitsunterstützung ausgelaufen ist.

2. Alle zwei Jahre prüft und ändert die Agentur gegebenenfalls die Anforderungen gemäß Absatz 1 und übermittelt etwaige Änderungen in Form eines Vorschlags an die Kommission.

3. Die Kommission kann im Wege von Durchführungsrechtsakten festlegen, dass die vorgeschlagenen bzw. geänderten Anforderungen gemäß den Absätzen 1 und 2 allgemeine Gültigkeit in der Union haben. Diese Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 55 Absatz 2 erlassen.

4. Die Kommission trägt dafür Sorge, dass die Anforderungen, denen gemäß Absatz 3 allgemeine Gültigkeit zuerkannt wurde, in geeigneter Weise veröffentlicht werden.

5. Die Agentur nimmt alle vorgeschlagenen Anforderungen bzw. deren genehmigte Änderungen in ein Register auf und veröffentlicht sie in geeigneter Weise.

Begründung

Aus Gründen der Klarheit sollte der Änderungsantrag des Entwurfs einer Stellungnahme in Buchstabe c geändert werden. 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 123
Cornelia Ernst

Vorschlag für eine Verordnung
Artikel 48 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	Artikel 48a
	Mindestanforderungen für IT-Sicherheit
	1. Die Agentur schlägt der Kommission bis [zwei Jahre nach Inkrafttreten der Verordnung] klare obligatorische Mindestsicherheitsanforderungen für alle IT-Geräte vor, die in der Union verkauft oder aus der Union ausgeführt werden, darunter folgende Anforderungen:
	(a) Der Anbieter legt eine schriftliche rechtlich bindende Bescheinigung darüber vor, dass das Gerät keine Hardware, Software oder Firmware mit bekannten Sicherheitslücken enthält.
	(b) Das Gerät ist mit Software bzw. Firmware ausgestattet, die vom Anbieter bereitgestellte ordnungsgemäß authentifizierte und aus vertrauenswürdiger Quelle stammende Aktualisierungen ermöglicht.
	(c) Das Gerät enthält keine unveränderlichen oder hartcodierten Anmeldeinformationen für die Fernverwaltung, die Bereitstellung von Aktualisierungen oder die

Kommunikation.

(d) Der Anbieter von internetfähigen Geräten, internetfähiger Software oder Firmware ist verpflichtet, den zuständigen Behörden alle bekannten Sicherheitslücken zu melden.

(e) Der Anbieter von internetfähigen Geräten, internetfähiger Software oder Firmware ist verpflichtet, eine Reparatur oder einen Ersatz anzubieten, wenn eine neue Sicherheitslücke entdeckt wird.

(f) Der Anbieter von internetfähigen Geräten, internetfähiger Software oder Firmware ist verpflichtet, darüber zu informieren, wie die Geräte Aktualisierungen erhalten und wann die Sicherheitsunterstützung planmäßig ausläuft, und wie förmlich mitgeteilt wird, dass eine solche Sicherheitsunterstützung ausgelaufen ist.

2. Alle zwei Jahre prüft und ändert die Agentur gegebenenfalls die Anforderungen gemäß Absatz 1 und übermittelt etwaige Änderungen in Form eines Vorschlags an die Kommission.

3. Die Kommission legt im Wege von Durchführungsrechtsakten fest, dass die vorgeschlagenen bzw. geänderten Anforderungen gemäß den Absätzen 1 und 2 allgemeine Gültigkeit in der Union haben. Diese Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren gemäß Artikel 55 Absatz 2 erlassen.

4. Die Kommission trägt dafür Sorge, dass die Anforderungen, denen gemäß Absatz 3 allgemeine Gültigkeit zuerkannt wurde, in geeigneter Weise veröffentlicht werden.

5. Die Agentur nimmt alle vorgeschlagenen Anforderungen bzw. deren genehmigte Änderungen in ein Register auf und veröffentlicht sie in geeigneter Weise.

Begründung

Damit soll der Vorschlag des Berichterstatters geringfügig verbessert werden.

Änderungsantrag 124
Daniel Dalton

Vorschlag für eine Verordnung
Artikel 48 a (neu)

Vorschlag der Kommission	*Geänderter Text*
	Artikel 48a
	Grundanforderungen im Bereich der IT-Sicherheit
	1. Die Agentur schlägt der Kommission bis [zwei Jahre nach Inkrafttreten der Verordnung] klare Grundanforderungen im Bereich der IT-Sicherheit für alle IT-Geräte vor, die in der Union verkauft oder aus der Union ausgeführt werden, zu deren allgemeiner Einhaltung, wo angebracht, die Branche angehalten werden sollte, darunter folgende Anforderungen:
	(a) Der Anbieter legt eine schriftliche Bescheinigung darüber vor, dass das Gerät keine Hardware, Software oder Firmware mit bekannten Sicherheitslücken enthält.
	(b) Das Gerät ist mit Software bzw. Firmware ausgestattet, die vom Anbieter bereitgestellte ordnungsgemäß authentifizierte und aus vertrauenswürdiger Quelle stammende Aktualisierungen ermöglicht.
	(c) Das Gerät enthält kein unverschlüsseltes Kennwort bzw. unverschlüsselten Zugangscode. Es wird jedoch die Verwendung sicherer Elemente für die Fernverwaltung, die Bereitstellung von Aktualisierungen oder die Kommunikation nachdrücklich

empfohlen.

(d) Der Anbieter von Geräten, Software oder Firmware, die mit dem Internet verbunden sind, ist verpflichtet, den zuständigen Behörden alle bekannten Sicherheitslücken zu melden.

(e) Der Anbieter von Geräten, Software oder Firmware, die mit dem Internet verbunden sind, ist verpflichtet, eine Reparatur oder einen Ersatz anzubieten, wenn eine neue Sicherheitslücke entdeckt wird.

(f) Der Anbieter von Geräten, Software oder Firmware, die mit dem Internet verbunden sind, ist verpflichtet, darüber zu informieren, wie die Geräte Aktualisierungen erhalten und wann die Sicherheitsunterstützung planmäßig ausläuft, und wie förmlich mitgeteilt wird, dass eine solche Sicherheitsunterstützung ausgelaufen ist.

2. Alle zwei Jahre prüft und ändert die Agentur gegebenenfalls die Anforderungen gemäß Absatz 1 und übermittelt etwaige Änderungen in Form eines Vorschlags an die Kommission.

Or. en

Begründung

Der Vorschlag des Berichterstatters wird geändert, damit die Grundanforderungen im Bereich der IT-Sicherheit freiwillig sind und dort angewendet werden, wo dies angebracht ist. Der Buchstabe c des Vorschlags des Berichterstatters wurde missverständlich formuliert. Während unverschlüsselte Anmeldeinformationen zu einem geringeren Schutz führen, bietet die Verwendung hartcodierter Daten in Geräten, etwa bei sicheren Komponenten, zusätzlichen Schutz.

Änderungsantrag 125
Cornelia Ernst

Vorschlag für eine Verordnung
Artikel 50 – Absatz 6 – Buchstabe d

Vorschlag der Kommission	*Geänderter Text*
(d) Zusammenarbeit mit anderen nationalen Aufsichtsbehörden für die Zertifizierung und anderen öffentlichen Stellen; dies beinhaltet auch den Informationsaustausch über die etwaige Nichtkonformität von IKT-Produkten und -Diensten mit den Anforderungen dieser Verordnung oder bestimmten europäischen Systemen für die Cybersicherheitszertifizierung;	(d) Zusammenarbeit mit anderen nationalen Aufsichtsbehörden für die Zertifizierung und anderen öffentlichen Stellen***, etwa den nationalen Aufsichtsbehörden im Bereich des Datenschutzes***; dies beinhaltet auch den Informationsaustausch über die etwaige Nichtkonformität von IKT-Produkten und -Diensten mit den Anforderungen dieser Verordnung oder bestimmten europäischen Systemen für die Cybersicherheitszertifizierung;

Or. en

Begründung

Entsprechend der Stellungnahme des Europäischen Datenschutzbeauftragten.