



PARLAMENT EUROPEJSKI

2009 - 2014

Komisja Rynku Wewnętrznego i Ochrony Konsumentów

2013/0027(COD)

2.10.2013

POPRAWKI 106 - 232

Projekt sprawozdania
Andreas Schwab
(PE514.882v01)

w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii

Wniosek dotyczący dyrektywy
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

AM\1004135PL.doc

PE519.685v01-00

PL

Zjednoczona w różnorodności

PL

AM_Com_LegReport

PL

Poprawka 106
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Umocowanie 4 a (nowe)

Tekst proponowany przez Komisję

Poprawka

uwzględniając rezolucję Parlamentu Europejskiego z dnia 12 września 2013 r. w sprawie strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń,

Or. es

Poprawka 107
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Motyw –1 (nowy)

Tekst proponowany przez Komisję

Poprawka

(–1) W dzisiejszych czasach technologie informacyjno-komunikacyjne (ICT) powinny uwzględniać potrzeby społeczeństwa, w tym osób zagrożonych wykluczeniem społecznym. Wszyscy użytkownicy ICT mają prawo oczekiwać przestrzegania minimalnych norm gwarantujących wiarygodność, bezpieczeństwo, przejrzystość, prostotę, interoperacyjność oraz ograniczenie ryzyka w zakresie ICT.

Or. es

Poprawka 108
Zuzana Roithová

Wniosek dotyczący dyrektywy Motyw 2

Tekst proponowany przez Komisję

(2) Skala i częstotliwość umyślnych lub przypadkowych incydentów w obszarze bezpieczeństwa **stają się coraz większe** i stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. Incydenty takie mogą utrudniać prowadzenie działalności gospodarczej, powodować znaczne straty finansowe, podważać zaufanie użytkowników oraz powodować znaczne straty w gospodarce Unii.

Poprawka

(2) Skala i częstotliwość umyślnych lub przypadkowych incydentów w obszarze bezpieczeństwa **ogromnie wzrastają** i stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. Incydenty takie mogą utrudniać prowadzenie działalności gospodarczej, powodować znaczne straty finansowe, podważać zaufanie **i naruszać prywatność** użytkowników, **podstawowe prawa i swobody obywateli Unii** oraz powodować znaczne straty w gospodarce Unii.

Or. cs

Poprawka 109 Zuzana Roithová

Wniosek dotyczący dyrektywy Motyw 3

Tekst proponowany przez Komisję

(3) Jako ponadgraniczne narzędzia komunikacji cyfrowe systemy informatyczne, a przede wszystkim internet, odgrywają istotną rolę w ułatwianiu transgranicznego przepływu towarów, usług **i osób**. Ze względu na ponadnarodowy charakter tych narzędzi poważne zakłócenia systemów w jednym państwie członkowskim mogą mieć wpływ na pozostałe państwa członkowskie oraz na Unię jako całość. Odporność **i** stabilność sieci i systemów informatycznych mają zatem zasadnicze znaczenie dla zapewnienia sprawnego funkcjonowania rynku wewnętrznego.

Poprawka

(3) Jako ponadgraniczne narzędzia komunikacji cyfrowe systemy informatyczne, a przede wszystkim internet, odgrywają istotną rolę w ułatwianiu transgranicznego przepływu towarów, usług, osób **i kapitału**. Ze względu na ponadnarodowy charakter tych narzędzi poważne zakłócenia systemów w jednym państwie członkowskim mogą mieć wpływ na pozostałe państwa członkowskie oraz na Unię jako całość. Odporność, stabilność **i wzajemne powiązania** sieci i systemów informatycznych mają zatem zasadnicze znaczenie dla zapewnienia sprawnego funkcjonowania rynku wewnętrznego.

Poprawka 110
Christian Engström

Wniosek dotyczący dyrektywy
Motyw 3 a (nowy)

Tekst proponowany przez Komisję

Poprawka

(3a) Ponieważ do awarii systemów najczęściej dochodzi nadal z przyczyn niezamierzonych, takich jak przyczyny naturalne lub błąd ludzki, infrastruktura powinna być odporna na zakłócenia zarówno zamierzone, jak i niezamierzone, a operatorzy infrastruktury krytycznej powinni projektować systemy oparte na zasadzie odporności, które nadal działają nawet w razie awarii innych systemów poza ich kontrolą.

Or. en

Poprawka 111
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Motyw 3 a (nowy)

Tekst proponowany przez Komisję

Poprawka

(3a) Bezpieczeństwo sieci i informacji w Unii Europejskiej powinno umożliwić istnienie bezpiecznego i wiarygodnego środowiska cyfrowego przy jednoczesnym zagwarantowaniu neutralności sieci i powszechnego prawa dostępu do technologii i wszelkich powiązanych usług. Bezpieczeństwo cybernetyczne powinno posiadać regulacje wykluczające jakiegokolwiek działania uznaniowe.

Poprawka 112
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Motyw 5

Tekst proponowany przez Komisję

(5) W celu uwzględnienia wszystkich istotnych incydentów i zagrożeń niniejsza dyrektywa powinna mieć zastosowanie do wszystkich sieci i systemów informatycznych. ***Obowiązki nałożone na organy administracji publicznej i podmioty gospodarcze nie powinny mieć jednak zastosowania w odniesieniu do przedsiębiorstw udostępniających publiczne sieci łączności lub świadczących publicznie dostępne usługi łączności elektronicznej w rozumieniu dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa)²⁵, które podlegają szczególnym wymogom w zakresie bezpieczeństwa i integralności ustanowionym w art. 13a tej dyrektywy, ani nie powinny mieć zastosowania w odniesieniu do dostawców usług zaufania.***

Poprawka

(5) W celu uwzględnienia wszystkich istotnych incydentów i zagrożeń niniejsza dyrektywa powinna mieć zastosowanie do wszystkich sieci i systemów informatycznych.

Poprawka 113
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Motyw 5 a (nowy)

Tekst proponowany przez Komisję

Poprawka

(5a) Wiele państw członkowskich wciąż

nie opublikowało krajowych strategii w sprawie bezpieczeństwa cybernetycznego ani nie opracowało planów awaryjnych na wypadek incydentów cybernetycznych. Ponadto niektóre z nich nie powołały zespołu reagowania na incydenty komputerowe (CERT) ani nie ratyfikowały konwencji Rady Europy o cyberprzestępczości.

Or. es

Poprawka 114
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Motyw 6

Tekst proponowany przez Komisję

(6) Obecne zdolności nie są wystarczające w celu zapewnienia wysokiego poziomu bezpieczeństwa sieci i informacji w Unii. Państwa członkowskie bardzo się różnią pod względem poziomu gotowości, co powoduje rozdrobnienie podejścia w obrębie Unii. Prowadzi to do nierównego poziomu ochrony konsumentów i przedsiębiorstw oraz negatywnie wpływa na ogólny poziom bezpieczeństwa sieci i informacji w Unii. Brak wspólnych minimalnych wymogów dla organów administracji publicznej i podmiotów gospodarczych uniemożliwia z kolei ustanowienie globalnego i skutecznego mechanizmu współpracy na poziomie Unii.

Poprawka

(6) Obecne zdolności nie są wystarczające w celu zapewnienia wysokiego poziomu bezpieczeństwa sieci i informacji w Unii. Państwa członkowskie bardzo się różnią pod względem poziomu gotowości, co powoduje rozdrobnienie podejścia w obrębie Unii. Prowadzi to do nierównego poziomu ochrony konsumentów i przedsiębiorstw oraz negatywnie wpływa na ogólny poziom bezpieczeństwa sieci i informacji w Unii. Brak wspólnych minimalnych wymogów dla organów administracji publicznej i podmiotów gospodarczych uniemożliwia z kolei ustanowienie globalnego i skutecznego mechanizmu współpracy na poziomie Unii. ***Konieczna jest skuteczna stymulacja działalności badawczej, rozwojowej i innowacyjnej w tej dziedzinie przy zastosowaniu odpowiednich środków finansowych. Uniwersytety i placówki badawcze odgrywają zasadniczą rolę w tym zakresie.***

Or. es

Poprawka 115
Andreas Schwab

Wniosek dotyczący dyrektywy
Motyw 8

Tekst proponowany przez Komisję

(8) Przepisy niniejszej dyrektywy nie powinny naruszać przysługujących każdemu państwu członkowskiemu praw do wprowadzania niezbędnych środków w celu zapewnienia ochrony podstawowych interesów w zakresie bezpieczeństwa narodowego, do ochrony porządku publicznego i bezpieczeństwa publicznego oraz do zezwalania na prowadzenie dochodzeń dotyczących przestępstw karnych oraz na ich wykrywanie i ściganie. Zgodnie z art. 346 TFUE żadne państwo członkowskie nie ma obowiązku udzielania informacji, których ujawnienie uznaje za sprzeczne z podstawowymi interesami jego bezpieczeństwa.

Poprawka

(8) Przepisy niniejszej dyrektywy nie powinny naruszać przysługujących każdemu państwu członkowskiemu praw do wprowadzania niezbędnych środków w celu zapewnienia ochrony podstawowych interesów w zakresie bezpieczeństwa narodowego, do ochrony porządku publicznego i bezpieczeństwa publicznego oraz do zezwalania na prowadzenie dochodzeń dotyczących przestępstw karnych oraz na ich wykrywanie i ściganie. Zgodnie z art. 346 TFUE żadne państwo członkowskie nie ma obowiązku udzielania informacji, których ujawnienie uznaje za sprzeczne z podstawowymi interesami jego bezpieczeństwa. ***Żadne państwo członkowskie nie ma obowiązku ujawniania niejawnych informacji UE zgodnie z decyzją Rady z dnia 31 marca 2011 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (2011/292/UE), informacji objętych postanowieniami umów o zachowaniu poufności lub nieformalnych umów o zachowaniu poufności, takich jak protokół TLP.***

Or. en

Uzasadnienie

Celem niniejszej poprawki jest doprecyzowanie sposobu przetwarzania informacji poufnych w ramach zakresu stosowania niniejszej dyrektywy.

Poprawka 116
Andreas Schwab

Wniosek dotyczący dyrektywy
Motyw 10 a (nowy)

Tekst proponowany przez Komisję

Poprawka

(10a) Z uwagi na różnice w krajowych strukturach zarządzania oraz w celu zabezpieczenia obowiązujących już ustaleń sektorowych lub unijnych organów nadzorczych i regulacyjnych, a także w celu unikania powielania należy umożliwić państwom członkowskim wyznaczenie więcej niż jednego właściwego organu krajowego odpowiedzialnego za realizację zadań związanych z bezpieczeństwem sieci i systemów informatycznych podmiotów gospodarczych objętych niniejszą dyrektywą. Jednak w celu zapewnienia sprawnej współpracy i komunikacji transgranicznej konieczne jest, aby każde państwo członkowskie, bez uszczerbku dla sektorowych ustaleń regulacyjnych, wyznaczyło tylko jeden krajowy pojedynczy punkt kontaktowy odpowiedzialny za współpracę transgraniczną na szczeblu unijnym. Jeżeli wymaga tego struktura konstytucyjna lub inne ustalenia danego państwa członkowskiego, powinno mieć ono prawo do wyznaczenia tylko jednego organu, który będzie wykonywał zadania właściwego organu i pojedynczego punktu kontaktowego.

Or. en

Uzasadnienie

Niniejsza poprawka zastępuje poprawkę 5, a jej celem jest uwzględnienie istniejących sektorowych organów unijnych, które już zajmują się bezpieczeństwem sieci i informacji w niektórych sektorach.

Poprawka 117
Christian Engström

Wniosek dotyczący dyrektywy
Motyw 13 a (nowy)

Tekst proponowany przez Komisję

Poprawka

(13a) W stosownych przypadkach podczas stosowania przepisów niniejszej dyrektywy państwa członkowskie mogą wykorzystywać lub dostosowywać istniejące struktury organizacyjne . Podczas opracowywania krajowych strategii w zakresie bezpieczeństwa sieci i informacji należy przeprowadzać analizę i ocenę istniejących planów i procesów.

Or. en

Uzasadnienie

W państwach członkowskich trwają już godne polecenia działania w tej kwestii i takie struktury oraz fora powinny być zachowane lub w stosownych przypadkach dostosowane.

Poprawka 118
Christian Engström

Wniosek dotyczący dyrektywy
Motyw 14

Tekst proponowany przez Komisję

Poprawka

(14) Aby umożliwić wymianę szczególnie chronionych i poufnych informacji w ramach sieci współpracy, należy zapewnić bezpieczną infrastrukturę do wymiany informacji. Bez uszczerbku dla obowiązków związanych ze zgłaszaniem incydentów i zagrożeń o znaczeniu ogólnounijnym w ramach sieci współpracy, dostęp do informacji poufnych z innych państw członkowskich można przyznać wyłącznie tym państwom członkowskim, które wykazały, że ich zasoby i procedury

(14) Aby umożliwić wymianę szczególnie chronionych i poufnych informacji w ramach sieci współpracy, należy zapewnić bezpieczną infrastrukturę do wymiany informacji. ***Do tego celu mogłyby zostać wykorzystane bezpieczne ogólnoeuropejskie usługi telematyczne między administracjami (STESTA).*** Bez uszczerbku dla obowiązków związanych ze zgłaszaniem incydentów i zagrożeń o znaczeniu ogólnounijnym w ramach sieci współpracy, dostęp do informacji poufnych

techniczne i finansowe oraz zasoby ludzkie, jak również ich infrastruktura łączności, gwarantują ich skuteczne, sprawne i bezpieczne uczestnictwo w sieci.

z innych państw członkowskich można przyznać wyłącznie tym państwom członkowskim, które wykazały, że ich zasoby i procedury techniczne i finansowe oraz zasoby ludzkie, jak również ich infrastruktura łączności, gwarantują ich skuteczne, sprawne i bezpieczne uczestnictwo w sieci.

Or. en

Poprawka 119
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Motyw 14

Tekst proponowany przez Komisję

(14) Aby umożliwić wymianę szczególnie chronionych i poufnych informacji w ramach sieci współpracy, należy zapewnić bezpieczną infrastrukturę do wymiany informacji. Bez uszczerbku dla obowiązków związanych ze zgłaszaniem incydentów i zagrożeń o znaczeniu ogólnounijnym w ramach sieci współpracy, dostęp do informacji poufnych z innych państw członkowskich można przyznać wyłącznie tym państwom członkowskim, które wykazały, że ich zasoby i procedury techniczne i finansowe oraz zasoby ludzkie, jak również ich infrastruktura łączności, gwarantują ich skuteczne, sprawne i bezpieczne uczestnictwo w sieci.

Poprawka

(14) Aby umożliwić wymianę szczególnie chronionych i poufnych informacji w ramach sieci współpracy, należy zapewnić bezpieczną infrastrukturę do wymiany informacji. Bez uszczerbku dla obowiązków związanych ze zgłaszaniem incydentów i zagrożeń o znaczeniu ogólnounijnym w ramach sieci współpracy, dostęp do informacji poufnych z innych państw członkowskich można przyznać wyłącznie tym państwom członkowskim, które wykazały, że ich zasoby i procedury techniczne i finansowe oraz zasoby ludzkie, jak również ich infrastruktura łączności, gwarantują ich skuteczne, sprawne i bezpieczne uczestnictwo w sieci. ***Zawsze powinno się przy tym stosować przejrzyste metody wykluczające wszelką arbitralność pomiędzy państwami członkowskimi.***

Or. es

Poprawka 120
Christian Engström

Wniosek dotyczący dyrektywy
Motyw 16

Tekst proponowany przez Komisję

(16) W celu zapewnienia przejrzystości i w celu odpowiedniego informowania obywateli UE i podmiotów gospodarczych właściwe organy powinny założyć wspólną stronę internetową, na której publikowane będą niemające poufnego charakteru informacje na temat incydentów i zagrożeń.

Poprawka

(16) W celu zapewnienia przejrzystości i w celu odpowiedniego informowania obywateli UE i podmiotów gospodarczych właściwe organy powinny założyć wspólną stronę internetową, na której publikowane będą niemające poufnego charakteru informacje na temat incydentów i zagrożeń. ***Wszelkie dane osobowe publikowane na tej stronie internetowej powinny ograniczać się do tego, co niezbędne, i być jak najbardziej anonimowe.***

Or. en

Poprawka 121
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Motyw 16

Tekst proponowany przez Komisję

(16) W celu zapewnienia przejrzystości i w celu odpowiedniego informowania obywateli UE i podmiotów gospodarczych właściwe organy powinny ***założyć wspólną stronę internetową, na której publikowane będą*** niemające poufnego charakteru informacje na temat incydentów i zagrożeń.

Poprawka

(16) W celu zapewnienia przejrzystości i w celu odpowiedniego informowania obywateli UE i podmiotów gospodarczych właściwe organy powinny ***publikować*** niemające poufnego charakteru informacje na temat incydentów i zagrożeń ***w głównych przestrzeniach cyfrowych, w których podobnie jak na stronach internetowych możliwe jest wyszukiwanie informacji za pośrednictwem telefonów komórkowych i tabletów.***

Or. es

Poprawka 122
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Motyw 16 a (nowy)

Tekst proponowany przez Komisję

Poprawka

(16a) W tym zakresie należy uwzględnić zwłaszcza szczególnie wrażliwe sektory społeczne, takie jak obywatele dotknięci konsekwencjami przeпаści cyfrowej lub mniejszości korzystające z portali społecznościowych. Konieczny jest też szczególny wysiłek na rzecz podnoszenia świadomości i edukacji społeczeństwa. Państwa członkowskie powinny dołożyć starań, aby MŚP mogły pogłębić swą wiedzę na temat bezpieczeństwa sieci i informacji oraz zwiększyć swe zdolności w zakresie bezpieczeństwa cybernetycznego.

Or. es

Poprawka 123
Konstantinos Poupakis

Wniosek dotyczący dyrektywy
Motyw 18 a (nowy)

Tekst proponowany przez Komisję

Poprawka

(18a) W celu ułatwienia współpracy między państwami członkowskimi a Komisją w zakresie działań, które podejmują one w kontekście transgranicznym w zakresie zapobiegania, wykrywania i postępowania w przypadkach związanych z bezpieczeństwem sieci i informacji, ENISA powinna stworzyć i obsługiwać ogólnoeuropejski mechanizm wczesnego ostrzegania i reagowania, który byłby uzupełnieniem mechanizmów funkcjonujących w państwach

Uzasadnienie

Tam, gdzie w kwestii bezpieczeństwa w cyberprzestrzeni zaangażowane jest więcej niż jedno państwo członkowskie, ENISA powinna mieć możliwość interwencji, ogłaszając alarm na szczeblu europejskim, tak aby we współpracy z organami publicznymi oraz pojedynczymi punktami kontaktowymi państwa członkowskie mogły lepiej skoordynować mechanizmy reagowania.

Poprawka 124
Christian Engström

Wniosek dotyczący dyrektywy
Motyw 21

Tekst proponowany przez Komisję

(21) Ze względu na globalny charakter problemów związanych z bezpieczeństwem sieci i informacji istnieje potrzeba zacieśnienia współpracy międzynarodowej w celu poprawy norm bezpieczeństwa i wymiany informacji oraz w celu promowania wspólnego globalnego podejścia w zakresie bezpieczeństwa sieci i informacji.

Poprawka

(21) Ze względu na globalny charakter problemów związanych z bezpieczeństwem sieci i informacji istnieje potrzeba zacieśnienia współpracy międzynarodowej w celu poprawy norm bezpieczeństwa i wymiany informacji oraz w celu promowania wspólnego globalnego podejścia w zakresie bezpieczeństwa sieci i informacji. ***Wszelkie ramy takiej współpracy międzynarodowej powinny podlegać przepisom dyrektywy 95/46/WE i rozporządzenia (WE) nr 45/2001.***

Poprawka 125
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Motyw 27

Tekst proponowany przez Komisję

(27) Aby uniknąć nakładania nieproporcjonalnie dużych obciążeń finansowych i administracyjnych na małe podmioty i na małych użytkowników, wymogi powinny być proporcjonalne do zagrożenia związanego z daną siecią lub danym systemem informatycznym oraz powinny uwzględniać najnowszy stan wiedzy na temat tego rodzaju środków. Wymogi te nie powinny mieć zastosowania w odniesieniu do mikroprzedsiębiorstw.

Poprawka

(27) Aby uniknąć nakładania nieproporcjonalnie dużych obciążeń finansowych i administracyjnych na małe podmioty i na małych użytkowników, wymogi powinny być proporcjonalne do zagrożenia związanego z daną siecią lub danym systemem informatycznym oraz powinny uwzględniać najnowszy stan wiedzy na temat tego rodzaju środków. Wymogi te nie powinny mieć zastosowania w odniesieniu do mikroprzedsiębiorstw, ***którym należy udostępnić stosowny instrument finansowy stanowiący pomoc i umożliwiający spełnienie podanych wymogów.***

Or. es

Poprawka 126
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Motyw 28

Tekst proponowany przez Komisję

(28) Właściwe organy powinny zwracać należytą uwagę na zachowanie nieformalnych i bezpiecznych kanałów wymiany informacji między podmiotami gospodarczymi i między sektorami publicznym i prywatnym. Decyzje o informowaniu społeczeństwa o incydentach zgłoszonych właściwym organom należy podejmować przy zachowaniu równowagi między interesem publicznym, zgodnie z którym społeczeństwo powinno być informowane o zagrożeniach, a ryzykiem utraty reputacji i poniesienia szkód handlowych, na jakie narażone są organy administracji publicznej i podmioty gospodarcze zgłaszające incydenty. Wykonując

Poprawka

(28) Właściwe organy powinny zwracać należytą uwagę na zachowanie nieformalnych i bezpiecznych kanałów wymiany informacji między podmiotami gospodarczymi i między sektorami publicznym i prywatnym. Decyzje o informowaniu społeczeństwa o incydentach zgłoszonych właściwym organom należy podejmować przy zachowaniu równowagi między interesem publicznym, zgodnie z którym społeczeństwo powinno być informowane o zagrożeniach, a ryzykiem utraty reputacji i poniesienia szkód handlowych, na jakie narażone są organy administracji publicznej i podmioty gospodarcze zgłaszające incydenty. Wykonując

obowiązki w zakresie powiadamiania, właściwe organy powinny zwracać szczególną uwagę na potrzebę zachowania poufności w odniesieniu do informacji dotyczących słabych punktów produktów, aż do momentu udostępnienia stosownych rozwiązań problemów bezpieczeństwa.

obowiązki w zakresie powiadamiania, właściwe organy powinny zwracać szczególną uwagę na potrzebę zachowania poufności w odniesieniu do informacji dotyczących słabych punktów produktów, aż do momentu udostępnienia stosownych rozwiązań problemów bezpieczeństwa. ***W żadnym wypadku nie mogą być ograniczane ani uchylane podstawowe prawa do informacji i komunikacji, na których opiera się państwo prawa.***

Or. es

Poprawka 127
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Motyw 29

Tekst proponowany przez Komisję

(29) Właściwe organy powinny dysponować niezbędnymi środkami do wykonywania swoich obowiązków, w tym uprawnieniami do uzyskiwania wystarczających informacji od podmiotów gospodarczych i organów administracji publicznej, w celu oceny poziomu bezpieczeństwa sieci i systemów informatycznych, jak również wiarygodnymi i pełnymi danymi na temat incydentów, które mają wpływ na funkcjonowanie sieci i systemów informatycznych.

Poprawka

(29) Właściwe organy powinny dysponować niezbędnymi środkami do wykonywania swoich obowiązków, w tym uprawnieniami do uzyskiwania wystarczających informacji od podmiotów gospodarczych i organów administracji publicznej, w celu oceny poziomu bezpieczeństwa sieci i systemów informatycznych, jak również wiarygodnymi i pełnymi danymi na temat incydentów, które mają wpływ na funkcjonowanie sieci i systemów informatycznych. ***Właściwe organy powinny mieć możliwość pociągnięcia do odpowiedzialności dostawców wadliwego oprogramowania, sprzętu lub usług przyczyniających się w sposób bezpośredni do powstawania incydentów w zakresie bezpieczeństwa sieci i informacji.***

Or. es

Poprawka 128
Konstantinos Poupakis

Wniosek dotyczący dyrektywy
Motyw 29

Tekst proponowany przez Komisję

(29) Właściwe organy powinny dysponować niezbędnymi środkami do wykonywania swoich obowiązków, w tym uprawnieniami do uzyskiwania wystarczających informacji od podmiotów gospodarczych i organów administracji publicznej, w celu oceny poziomu bezpieczeństwa sieci i systemów informatycznych, jak również wiarygodnymi i pełnymi danymi na temat incydentów, które mają wpływ na funkcjonowanie sieci i systemów informatycznych.

Poprawka

(29) Właściwe organy, **pojedyncze punkty kontaktowe oraz ENISA** powinny dysponować niezbędnymi środkami do wykonywania swoich obowiązków, w tym uprawnieniami do uzyskiwania wystarczających informacji od podmiotów gospodarczych i organów administracji publicznej, w celu oceny poziomu bezpieczeństwa sieci i systemów informatycznych, jak również wiarygodnymi i pełnymi danymi na temat incydentów, które mają wpływ na funkcjonowanie sieci i systemów informatycznych.

Or. el

Poprawka 129
Konstantinos Poupakis

Wniosek dotyczący dyrektywy
Motyw 30

Tekst proponowany przez Komisję

(30) Źródłem incydentu w wielu przypadkach jest działalność przestępcza. Przestępczy charakter incydentów można podejrzewać nawet wtedy, gdy początkowo dowody nie są wystarczająco przekonujące. W tym kontekście odpowiednia współpraca między właściwymi organami i organami ścigania powinna stanowić część skutecznej i kompleksowej reakcji na zagrożenie związane z możliwością wystąpienia incydentu zagrażającego bezpieczeństwu. Wspieranie rozwoju bezpiecznego,

Poprawka

(30) Źródłem incydentu w wielu przypadkach jest działalność przestępcza. Przestępczy charakter incydentów można podejrzewać nawet wtedy, gdy początkowo dowody nie są wystarczająco przekonujące. W tym kontekście odpowiednia współpraca między właściwymi organami, **pojedynczymi punktami kontaktowymi, ENISA** i organami ścigania powinna stanowić część skutecznej i kompleksowej reakcji na zagrożenie związane z możliwością wystąpienia incydentu zagrażającego

chronionego i bardziej odpornego środowiska wymaga w szczególności systematycznego zgłaszania organom ścigania poważnych incydentów, które mogą mieć charakter przestępczy. Poważne incydenty o charakterze przestępczym należy oceniać w świetle prawa UE w zakresie cyberprzestępczości.

bezpieczeństwu. Wspieranie rozwoju bezpiecznego, chronionego i bardziej odpornego środowiska wymaga w szczególności systematycznego zgłaszania organom ścigania poważnych incydentów, które mogą mieć charakter przestępczy. Poważne incydenty o charakterze przestępczym należy oceniać w świetle prawa UE w zakresie cyberprzestępczości.

Or. el

Poprawka 130
Christian Engström

Wniosek dotyczący dyrektywy
Motyw 30 a (nowy)

Tekst proponowany przez Komisję

Poprawka

(30a) Niniejsza dyrektywa nie narusza unijnego dorobku prawnego dotyczącego ochrony danych.

Wszelkie dane osobowe wykorzystywane zgodnie z przepisami niniejszej dyrektywy powinny być ograniczone do tego, co jest absolutnie niezbędne, i przekazywane wyłącznie podmiotom, którym są absolutnie niezbędne, a także powinny być anonimowe, jeśli nie zupełnie, to w jak największym stopniu.

Or. en

Poprawka 131
Christian Engström

Wniosek dotyczący dyrektywy
Motyw 30 b (nowy)

Tekst proponowany przez Komisję

Poprawka

(30b) Przed przyjęciem na szczeblu UE przepisów dotyczących bezpieczeństwa

cybernetycznego należy przyjąć na tym szczeblu ogólne przepisy dotyczące ochrony danych. W związku z tym niniejszą dyrektywę należy przyjąć dopiero po przyjęciu ogólnego rozporządzenia o ochronie danych.

Or. en

Poprawka 132
Christian Engström

Wniosek dotyczący dyrektywy
Motyw 31

Tekst proponowany przez Komisję

(31) W wyniku incydentów w wielu przypadkach istnieje niebezpieczeństwo naruszenia danych osobowych. W tym kontekście właściwe organy **oraz organy ochrony danych** powinny ze sobą współpracować i wymieniać się informacjami **dotyczącymi wszystkich istotnych kwestii** w celu rozwiązywania problemów związanych z przypadkami naruszeń danych osobowych w wyniku incydentów. Państwa członkowskie powinny wdrożyć obowiązek zgłaszania incydentów zagrażających bezpieczeństwu w sposób, który minimalizuje obciążenia administracyjne w przypadku, gdy incydent zagrażający bezpieczeństwu stanowi również naruszenie danych osobowych w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Współpracując z właściwymi organami i organami ochrony danych, ENISA mogłaby opracować mechanizmy i wzory formularzy na potrzeby wymiany informacji, dzięki czemu nie byłoby konieczne stosowanie dwóch formularzy. Pojedynczy formularz ułatwiłby zgłaszanie

Poprawka

(31) W wyniku incydentów w wielu przypadkach istnieje niebezpieczeństwo naruszenia danych osobowych. W tym kontekście właściwe organy powinny ze sobą współpracować i wymieniać się informacjami, **w stosownych przypadkach z podmiotami gospodarczymi**, w celu rozwiązywania problemów związanych z przypadkami naruszeń danych osobowych w wyniku incydentów **zgodnie z mającymi zastosowanie przepisami w dziedzinie ochrony danych**. Państwa członkowskie powinny wdrożyć obowiązek zgłaszania incydentów zagrażających bezpieczeństwu w sposób, który minimalizuje obciążenia administracyjne w przypadku, gdy incydent zagrażający bezpieczeństwu stanowi również naruszenie danych osobowych w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Współpracując z właściwymi organami i organami ochrony danych, ENISA mogłaby opracować mechanizmy i wzory formularzy na potrzeby wymiany informacji, dzięki czemu nie byłoby konieczne stosowanie dwóch formularzy.

incydentów, które stanowią naruszenie danych osobowych, zmniejszając tym samym obciążenia administracyjne dla przedsiębiorstw i organów administracji publicznej.

Pojedynczy formularz ułatwiłby zgłaszanie incydentów, które stanowią naruszenie danych osobowych, zmniejszając tym samym obciążenia administracyjne dla przedsiębiorstw i organów administracji publicznej.

Or. en

Poprawka 133 Andreas Schwab

Wniosek dotyczący dyrektywy Motyw 34

Tekst proponowany przez Komisję

(34) W celu umożliwienia prawidłowego funkcjonowania sieci współpracy należy przekazać Komisji uprawnienia do przyjęcia aktów zgodnie z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej w odniesieniu do **określenia kryteriów, które państwo członkowskie musi spełnić, aby móc uczestniczyć w bezpiecznym systemie wymiany informacji, sprecyzowania**, które zdarzenia wymagają wczesnego ostrzegania, **a także określenia okoliczności, w których podmioty gospodarcze i organy administracji publicznej są zobowiązane do zgłaszania incydentów.**

Poprawka

(34) W celu umożliwienia prawidłowego funkcjonowania sieci współpracy należy przekazać Komisji uprawnienia do przyjęcia aktów zgodnie z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej w odniesieniu do **precyzowania**, które zdarzenia wymagają wczesnego ostrzegania.

Or. en

Uzasadnienie

Niniejsza poprawka zastępuje poprawkę 17 i jest powiązana z zaproponowanymi przez sprawozdawcę nowymi poprawkami do art. 9, 10 i 18 (zob. także uzasadnienie w odniesieniu do art. 18).

Poprawka 134 Andreas Schwab

Wniosek dotyczący dyrektywy Motyw 36

Tekst proponowany przez Komisję

(36) W celu zapewnienia jednolitych warunków wykonywania niniejszej dyrektywy należy powierzyć Komisji uprawnienia wykonawcze w zakresie współpracy między **właściwymi organami** i Komisją w ramach sieci współpracy, **dostępu do** bezpiecznej infrastruktury służącej do wymiany informacji, unijnego planu współpracy w zakresie bezpieczeństwa sieci i informacji, formatów i procedur mających zastosowanie wobec wymogów dotyczących **informowania społeczeństwa o incydentach, oraz norm lub specyfikacji technicznych dotyczących bezpieczeństwa sieci i informacji**. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiającym przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję.

Poprawka

(36) W celu zapewnienia jednolitych warunków wykonywania niniejszej dyrektywy należy powierzyć Komisji uprawnienia wykonawcze w zakresie współpracy między **pojedynczymi punktami kontaktowymi** i Komisją w ramach sieci współpracy, **bez uszczerbku dla istniejących mechanizmów współpracy na szczeblu krajowym, wspólnego zestawu norm w zakresie wzajemnych połączeń i bezpieczeństwa dla potrzeb** bezpiecznej infrastruktury służącej do wymiany informacji, unijnego planu współpracy w zakresie bezpieczeństwa sieci i informacji, **a także** formatów i procedur mających zastosowanie wobec wymogów dotyczących **zgłaszania incydentów mających znaczące konsekwencje**. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiającym przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję.

Or. en

Uzasadnienie

Niniejsza poprawka zastępuje poprawkę 20. Celem poprawki jest skorygowanie błędu, który pojawił się we wniosku Komisji w odniesieniu do treści planowanego aktu wykonawczego, oraz odzwierciedlenie nowej poprawki zaproponowanej w odniesieniu do art. 9 ust. 3.

Poprawka 135 Vicente Miguel Garcés Ramón

**Wniosek dotyczący dyrektywy
Motyw 37**

Tekst proponowany przez Komisję

(37) Przy stosowaniu niniejszej dyrektywy Komisja powinna w stosownych przypadkach współpracować z odpowiednimi komitetami sektorowymi i odpowiednimi organami ustanowionymi na poziomie UE, zwłaszcza w dziedzinie energetyki, transportu *i* opieki zdrowotnej.

Poprawka

(37) Przy stosowaniu niniejszej dyrektywy Komisja powinna w stosownych przypadkach współpracować z odpowiednimi komitetami sektorowymi i odpowiednimi organami ustanowionymi na poziomie UE, zwłaszcza w dziedzinie energetyki, transportu, opieki zdrowotnej *i sił wojskowych*.

Or. es

**Poprawka 136
Vicente Miguel Garcés Ramón**

**Wniosek dotyczący dyrektywy
Motyw 40 a (nowy)**

Tekst proponowany przez Komisję

Poprawka

(40a) Walce z cyberprzestępczością powinna towarzyszyć walka ze szpiegostwem pomiędzy państwami, naruszającym suwerenność UE i jej państw członkowskich. Niniejsza dyrektywa ma na celu ochronę obywateli, przedsiębiorstw, instytucji publicznych i prywatnych, jak również państw i rządów przed pospolitymi przestępcami, zorganizowanymi grupami przestępczymi i szpiegostwem, a także przed innego rodzaju cyberprzestępczością.

Or. es

**Poprawka 137
Vicente Miguel Garcés Ramón**

**Wniosek dotyczący dyrektywy
Motyw 41**

Tekst proponowany przez Komisję

(41) Niniejsza dyrektywa **jest zgodna z prawami podstawowymi i zasadami uznanymi** w Karcie praw podstawowych Unii Europejskiej, a w szczególności **zasadami dotyczącymi** prawa do poszanowania życia prywatnego i **komunikowania się**, prawa do ochrony danych **osobowych** i wolności prowadzenia działalności gospodarczej, prawa własności, prawa do skutecznego środka prawnego i prawa do bycia wysłuchanym. Niniejszą dyrektywę należy wdrażać zgodnie z tymi prawami i zasadami,

Poprawka

(41) Niniejsza dyrektywa **w żadnym wypadku nie powinna ograniczać ani uchylać praw podstawowych i zasad uznanych** w Karcie praw podstawowych Unii Europejskiej, a w szczególności **zasad dotyczących** prawa do poszanowania życia prywatnego, **prawa do informacji i komunikacji**, prawa do ochrony danych i wolności prowadzenia działalności gospodarczej, prawa własności, prawa do skutecznego środka prawnego i prawa do bycia wysłuchanym. Niniejszą dyrektywę należy wdrażać zgodnie z tymi prawami i zasadami,

Or. es

Poprawka 138 **Vicente Miguel Garcés Ramón**

Wniosek dotyczący dyrektywy **Artykuł 1 – ustęp 1**

Tekst proponowany przez Komisję

1. Niniejsza dyrektywa ustanawia środki w celu zapewnienia wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii.

Poprawka

1. Niniejsza dyrektywa ustanawia środki w celu zapewnienia wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii, **oferując bezpieczne i wiarygodne środowisko cyfrowe przy jednoczesnym zagwarantowaniu neutralności sieci i powszechnego prawa dostępu do telekomunikacji i wszelkich powiązanych usług.**

Or. es

Poprawka 139 **Vicente Miguel Garcés Ramón**

Wniosek dotyczący dyrektywy
Artykuł 1 – ustęp 2 – litera c

Tekst proponowany przez Komisję

c) ustanawia wymogi w zakresie bezpieczeństwa dla podmiotów gospodarczych i organów administracji publicznej.

Poprawka

c) ustanawia wymogi w zakresie bezpieczeństwa dla podmiotów gospodarczych i organów administracji publicznej, **wykluczające jakiegokolwiek działania uznaniowe.**

Or. es

Poprawka 140
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 1 – ustęp 2 – litera c

Tekst proponowany przez Komisję

c) ustanawia wymogi w zakresie bezpieczeństwa dla podmiotów gospodarczych **i organów administracji publicznej.**

Poprawka

c) ustanawia wymogi w zakresie bezpieczeństwa dla podmiotów gospodarczych.

Or. en

Uzasadnienie

Dostosowanie w związku z ograniczeniem zakresu stosowania poprawki w odniesieniu do rozdziału IV. Organy administracji publicznej nie powinny być włączone do zakresu stosowania rozdziału IV, ponieważ ich znaczenie dla funkcjonowania rynku wewnętrznego jest ograniczone, a ze względu na swoją misję publiczną powinny działać z należytą starannością. W związku z tym nakładanie na nie takich samych obowiązków, jak ma to miejsce w przypadku podmiotów gospodarczych, nie byłoby właściwe.

Poprawka 141
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Artykuł 1 – ustęp 3

Tekst proponowany przez Komisję

Poprawka

3. Wymogi bezpieczeństwa przewidziane w art. 14 nie mają zastosowania do przedsiębiorstw udostępniających publiczne sieci łączności lub świadczących publicznie dostępne usługi łączności elektronicznej w rozumieniu dyrektywy 2002/21/WE, które to przedsiębiorstwa muszą spełniać szczególne wymogi w zakresie bezpieczeństwa i integralności określone w art. 13a i 13b tej dyrektywy, ani do dostawców usług zaufania.

skreślony

Or. es

Poprawka 142
Christian Engström

Wniosek dotyczący dyrektywy
Artykuł 1 – ustęp 5

Tekst proponowany przez Komisję

Poprawka

5. Niniejsza dyrektywa pozostaje również bez uszczerbku dla dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym **przepływem** takich danych.

5. Niniejsza dyrektywa pozostaje również bez uszczerbku dla dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenia **(WE) nr 45/2001** Parlamentu Europejskiego i Rady z **dnia 18 grudnia 2000 r. o ochronie** osób fizycznych w związku z przetwarzaniem danych osobowych **przez instytucje i organy wspólnotowe** i o swobodnym **przepływie** takich danych. **Wszelkie wykorzystanie danych osobowych powinno być ograniczone do tego, co jest absolutnie niezbędne dla**

celów niniejszej dyrektywy, a dane te powinny być anonimowe, jeśli nie zupełnie, to w jak największym stopniu.

Or. en

Poprawka 143
Toine Manders

Wniosek dotyczący dyrektywy
Artykuł 1 – ustęp 6

Tekst proponowany przez Komisję

6. Wymiana informacji w ramach sieci współpracy na mocy rozdziału III i zgłaszanie incydentów dotyczących bezpieczeństwa sieci i informacji na mocy art. 14 mogą wymagać przetwarzania danych osobowych. Państwo członkowskie zezwala na takie przetwarzanie, które jest niezbędne do realizacji celów niniejszej dyrektywy będących w interesie publicznym, zgodnie z ustawodawstwem krajowym implementującym art. 7 dyrektywy 95/46/WE i dyrektywę 2002/58/WE.

Poprawka

6. Wymiana informacji w ramach sieci współpracy na mocy rozdziału III i zgłaszanie incydentów dotyczących bezpieczeństwa sieci i informacji na mocy art. 14 mogą wymagać przetwarzania danych osobowych. Państwo członkowskie zezwala na takie przetwarzanie, które jest niezbędne do realizacji celów niniejszej dyrektywy będących w interesie publicznym, zgodnie z ustawodawstwem krajowym implementującym art. 7 dyrektywy 95/46/WE i dyrektywę 2002/58/WE. ***Państwa członkowskie zapewniają, że podmioty gospodarcze i właściwe organy nie są pociągane do odpowiedzialności za wykorzystywanie danych osobowych wymaganych dla potrzeb wymiany informacji w ramach sieci współpracy.***

Or. en

Poprawka 144
Toine Manders

Wniosek dotyczący dyrektywy
Artykuł 2

Tekst proponowany przez Komisję

Państwa członkowskie **mają prawo przyjmowania** lub **utrzymania** w mocy **przepisów zapewniających** wyższy poziom bezpieczeństwa, **bez uszczerbku dla** ich zobowiązań wynikających z prawa unijnego.

Poprawka

Państwa członkowskie **przyjmują** lub **utrzymują** w mocy **przepisy zapewniające** wyższy poziom bezpieczeństwa, z **możliwością naruszenia** ich zobowiązań wynikających z prawa unijnego **i krajowych celów w dziedzinie bezpieczeństwa**.

Or. en

Poprawka 145
Christian Engström

Wniosek dotyczący dyrektywy
Artykuł 3 – punkt 2 a (nowy)

Tekst proponowany przez Komisję

Poprawka 146
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 3 – punkt 3

Tekst proponowany przez Komisję

3) „zagrożenie” oznacza każdą okoliczność lub zdarzenie, które mogą mieć niekorzystny wpływ na bezpieczeństwo;

Poprawka

2a) „odporność na zagrożenia cybernetyczne” oznacza zdolność sieci i systemów informatycznych do oparcia się zagrożeniu i powrotu do pełnej zdolności operacyjnej po incydentach, w tym – między innymi – takich jak niesprawność techniczna, awaria zasilania lub incydenty zagrażające bezpieczeństwu;

Or. en

wpływ na bezpieczeństwo;

Or. en

Poprawka 147
Toine Manders

Wniosek dotyczący dyrektywy
Artykuł 3 – punkt 5

Tekst proponowany przez Komisję

Poprawka

**5) „usługi społeczeństwa informacyjnego”
oznaczają usługę w rozumieniu art. 1 pkt
2) dyrektywy 98/34/WE;**

skreślony

Or. en

Poprawka 148
Toine Manders

Wniosek dotyczący dyrektywy
Artykuł 3 – punkt 8 – litera a

Tekst proponowany przez Komisję

Poprawka

**a) dostawcę usług społeczeństwa
informacyjnego umożliwiających
świadczenie innych usług społeczeństwa
informacyjnego, których niewyczerpujący
wykaz zamieszczony jest w załączniku II;**

skreślona

Or. en

Poprawka 149
Christian Engström

Wniosek dotyczący dyrektywy
Artykuł 3 – punkt 8 – litera b

Tekst proponowany przez Komisję

b) operatora infrastruktury krytycznej, która ma zasadnicze znaczenie dla utrzymania **kluczowych działań gospodarczych i społecznych w dziedzinach energetyki, transportu, bankowości, obrotu papierami wartościowymi i opieki zdrowotnej**, których niewyczerpujący wykaz zamieszczony jest w załączniku II.

Poprawka

b) operatora infrastruktury krytycznej, która ma zasadnicze znaczenie dla utrzymania **stabilności i odporności gospodarczej, zdrowia publicznego, bezpieczeństwa publicznego lub ich jakiegokolwiek połączenia, a której uszkodzenie lub zniszczenie miałyby znaczące konsekwencje dla danego państwa członkowskiego w wyniku braku możliwości utrzymania tych funkcji**, których niewyczerpujący wykaz zamieszczony jest w załączniku II.

Or. en

Poprawka 150

Philippe Juvin, Marielle Gallo

**Wniosek dotyczący dyrektywy
Artykuł 3 – punkt 8 – litera b**

Tekst proponowany przez Komisję

b) operatora infrastruktury krytycznej, która ma zasadnicze znaczenie dla utrzymania kluczowych działań gospodarczych i społecznych w dziedzinach energetyki, transportu, bankowości, obrotu papierami wartościowymi i opieki zdrowotnej, których niewyczerpujący wykaz zamieszczony jest w załączniku II.

Poprawka

b) operatora infrastruktury krytycznej, która ma zasadnicze znaczenie dla utrzymania kluczowych działań gospodarczych i społecznych w dziedzinach energetyki, transportu, bankowości, obrotu papierami wartościowymi i opieki zdrowotnej, których niewyczerpujący wykaz zamieszczony jest w załączniku II, **o ile odnośne sieci i systemy informatyczne są bezpośrednio z nią związane.**

Or. en

Uzasadnienie

W miejsce czysto „sektorowego” podejścia należy wprowadzić podejście „infrastrukturalne”. Nie wszystkie sieci i systemy informatyczne należące do operatora infrastruktury krytycznej są bowiem „krytyczne” w sensie posiadania zasadniczego znaczenia dla utrzymania kluczowych

działań (np. sieci i systemy informatyczne związane z utrzymaniem wyposażenia). Zakresem stosowania niniejszej dyrektywy powinny być objęte wyłącznie te sieci i systemy informatyczne, które są bezpośrednio związane z infrastrukturą krytyczną.

Poprawka 151
Toine Manders

Wniosek dotyczący dyrektywy
Artykuł 3 – akapit pierwszy a (nowy)

Tekst proponowany przez Komisję

Poprawka

1a. „mikroprzedsiębiorstwo” – którego definicja została określona w art. 2 ust. 3 zalecenia Komisji 2003/361/WE z dnia 6 maja 2003 r.¹ dotyczącym definicji przedsiębiorstw mikro, małych i średnich – nie jest „podmiotem gospodarczym” w zakresie stosowania niniejszej definicji, chyba że działa jako jednostka zależna operatora infrastruktury krytycznej w rozumieniu akapitu pierwszego lit. b) niniejszego punktu.

¹ Dz.U. L 124 z 20.5.2003, s. 36.

Or. en

Poprawka 152
Andreas Schwab, Malcolm Harbour

Wniosek dotyczący dyrektywy
Artykuł 4

Tekst proponowany przez Komisję

Poprawka

Artykuł 4

skreślony

Zasada

Państwa członkowskie zapewniają wysoki poziom bezpieczeństwa sieci i systemów informatycznych na swoim terytorium

zgodnie z niniejszą dyrektywą.

Or. en

Uzasadnienie

Skreślenie niezbędne w celu uniknięcia powielania przepisów art. 1 ust. 1. Ponadto państwa członkowskie mogą wyłącznie zapewnić zgodność działań z wymogami określonymi w niniejszej dyrektywie. Ogólna zasada dotycząca zapewnienia wysokiego poziomu bezpieczeństwa nie jest wykonalna.

Poprawka 153
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Artykuł 4

Tekst proponowany przez Komisję

Państwa członkowskie zapewniają wysoki poziom bezpieczeństwa sieci i systemów informatycznych na swoim terytorium zgodnie z niniejszą dyrektywą.

Poprawka

Państwa członkowskie zapewniają wysoki poziom bezpieczeństwa sieci i systemów informatycznych na swoim terytorium zgodnie z niniejszą dyrektywą. ***Walce z cyberprzestępczością powinna towarzyszyć walka ze szpiegostwem pomiędzy państwami mającym na celu naruszenie suwerenności UE i jej państw członkowskich.***

Or. es

Poprawka 154
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 1 – litera e

Tekst proponowany przez Komisję

e) plany w zakresie badań i rozwoju oraz opis, w jaki sposób plany te odzwierciedlają wyznaczone priorytety.

Poprawka

e) plany w zakresie badań i rozwoju, ***w których uniwersytety i placówki badawcze odgrywają zasadniczą rolę***, oraz opis, w jaki sposób plany te odzwierciedlają

wyznaczone priorytety.

Or. es

Poprawka 155
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 1 – litera e a (nowa)

Tekst proponowany przez Komisję

Poprawka

ea) systemy jakości utworzone z najwyższą starannością oraz zmiany potrzebne do realizacji niniejszej dyrektywy i rozszerzenia jej zakresu. Wszelkie aplikacje powinny być opracowywane przy użyciu kodu wielokrotnego użytku i, w miarę możliwości, otwartego oprogramowania.

Or. es

Poprawka 156
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 2 – litera a

Tekst proponowany przez Komisję

Poprawka

a) opracowanie *planu oceny* zagrożeń *umożliwiającego określenie zagrożeń i* ocenę wpływu potencjalnych incydentów;

a) opracowanie *ram zarządzania ryzykiem w celu stworzenia metodyki obejmującej określenie zagrożeń, ustalenie stopnia ich ważności, ich ocenę i postępowanie w przypadku ich wystąpienia, ocenę wpływu potencjalnych incydentów i sposoby zapobiegania i kontroli, a także w celu określenia kryteriów wyboru możliwych środków zaradczych;*

Or. en

Uzasadnienie

Niniejsza poprawka zastępuje poprawkę 29. Propozycja Komisji byłaby rozwiązaniem zbyt daleko idącym w odniesieniu do kwestii bezpieczeństwa narodowego państw członkowskich, a także uczyniłaby plan współpracy niemożliwym do realizacji oraz zbyt złożonym, aby zapewnić jego skuteczność.

Poprawka 157 **Christian Engström**

Wniosek dotyczący dyrektywy **Artykuł 5 – ustęp 2 – litera a**

Tekst proponowany przez Komisję

a) opracowanie planu oceny zagrożeń umożliwiającego określenie zagrożeń i ocenę wpływu potencjalnych incydentów;

Poprawka

a) opracowanie planu oceny zagrożeń umożliwiającego określenie zagrożeń i ocenę wpływu potencjalnych incydentów;
co roku należy dokonywać przeglądu i aktualizacji tego planu;

Or. en

Poprawka 158 **Vicente Miguel Garcés Ramón**

Wniosek dotyczący dyrektywy **Artykuł 5 – ustęp 2 – litera d a (nowa)**

Tekst proponowany przez Komisję

Poprawka

da) publikacja w sieci kompendium zawierającego spis wszelkich instytucji spełniających określone w dyrektywie wymogi odnośnie do zarządzania ryzykiem i danymi, przy jednoczesnym zagwarantowaniu nieograniczonego prawa obywateli wszystkich państw członkowskich do informacji, stawiając zarazem wymóg opracowania programu przejrzystości w odniesieniu do zarządzania bezpieczeństwem sieci i informacji oraz procedur w tym zakresie.

Poprawka 159
Sari Essayah

Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 2 – litera d a (nowa)

Tekst proponowany przez Komisję

Poprawka

da) poprawa warunków przechowywania i wykorzystywania haseł uwierzytelniających, na przykład poprzez większe wykorzystanie funkcji skrótu lub narzędzi zarządzania hasłami.

Or. en

Poprawka 160
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 2 – litera d b (nowa)

Tekst proponowany przez Komisję

Poprawka

db) uwzględnienie zwłaszcza szczególnie wrażliwych sektorów społecznych, takich jak obywatele dotknięci konsekwencjami przepaści cyfrowej lub mniejszości korzystające z portali społecznościowych.

Or. es

Poprawka 161
Christian Engström

Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 3

Tekst proponowany przez Komisję

3. Krajową strategię w zakresie bezpieczeństwa sieci i informacji oraz krajowy plan współpracy w zakresie bezpieczeństwa sieci i informacji są przekazywane Komisji w ciągu **jednego miesiąca** od ich przyjęcia.

Poprawka

3. Krajową strategię w zakresie bezpieczeństwa sieci i informacji oraz krajowy plan współpracy w zakresie bezpieczeństwa sieci i informacji są przekazywane Komisji w ciągu **trzech miesięcy** od ich przyjęcia.

Or. en

Poprawka 162 **Andreas Schwab**

Wniosek dotyczący dyrektywy **Artykuł 6 – ustęp 1**

Tekst proponowany przez Komisję

1. Każde państwo członkowskie wyznacza właściwy organ krajowy ds. bezpieczeństwa sieci i systemów informatycznych („**właściwy organ**”).

Poprawka

1. Każde państwo członkowskie wyznacza **co najmniej jeden cywilny** właściwy organ krajowy ds. bezpieczeństwa sieci i systemów informatycznych (**zwany dalej „właściwym organem / właściwymi organami”**).

Or. en

Uzasadnienie

Niniejsza poprawka zastępuje poprawkę 32, a jej celem jest dalsze doprecyzowanie, jaki rodzaj instytucji powinien pełnić rolę właściwego organu krajowego.

Poprawka 163 **Vicente Miguel Garcés Ramón**

Wniosek dotyczący dyrektywy **Artykuł 6 – ustęp 2**

Tekst proponowany przez Komisję

2. Właściwe organy monitorują stosowanie niniejszej dyrektywy na poziomie

Poprawka

2. Właściwe organy monitorują stosowanie niniejszej dyrektywy na poziomie

krajowym oraz przyczyniają się do jej jednolitego stosowania w całej Unii.

krajowym oraz przyczyniają się do jej jednolitego stosowania w całej Unii.
Monitorują również stosowanie środków na rzecz bezpieczeństwa sieci i informacji objętych dyrektywą.

Or. es

Poprawka 164
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 6 – ustęp 2 a (nowy)

Tekst proponowany przez Komisję

Poprawka

2a. Jeżeli państwo członkowskie wyznacza więcej niż jeden właściwy organ, wyznacza ono krajowy organ cywilny, np. właściwy organ, jako pojedynczy krajowy punkt kontaktowy ds. bezpieczeństwa sieci i systemów informatycznych (zwany dalej „pojedynczym punktem kontaktowym”). Jeżeli państwo członkowskie wyznacza tylko jeden właściwy organ, organ ten jest również pojedynczym punktem kontaktowym.

Or. en

Uzasadnienie

Niniejsza poprawka zastępuje poprawkę 33 i stanowi dostosowanie do zaproponowanej przez sprawozdawcę nowej poprawki dotyczącej art. 6 ust. 1. Celem poprawki jest dalsze doprecyzowanie, jaki rodzaj instytucji powinien pełnić rolę pojedynczego punktu kontaktowego.

Poprawka 165
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 6 – ustęp 4

Tekst proponowany przez Komisję

4. Państwa członkowskie dopilnowują, by właściwe organy otrzymywały od **organów administracji publicznej i** podmiotów gospodarczych zgłoszenia dotyczące incydentów określone w art. 14 ust. 2 oraz posiadały uprawnienia w zakresie wykonywania i egzekwowania przepisów, o których mowa w art. 15.

Poprawka

4. Państwa członkowskie dopilnowują, by właściwe organy **i pojedyncze punkty kontaktowe – w stosownych przypadkach zgodnie z ust. 2a niniejszego artykułu –** otrzymywały od podmiotów gospodarczych zgłoszenia dotyczące incydentów określone w art. 14 ust. 2 oraz posiadały uprawnienia w zakresie wykonywania i egzekwowania przepisów, o których mowa w art. 15.

Or. en

Uzasadnienie

Niniejsza poprawka zastępuje poprawkę 37. Jej celem jest doprecyzowanie roli poszczególnych organów w celu zapobiegania powielaniu zgłoszeń adresowanych zarówno do właściwych organów, jak i do pojedynczych punktów kontaktowych. Biorąc pod uwagę, że w niektórych sektorach incydenty zgłaszane są już organom unijnym, należy unikać powielania tych zgłoszeń.

Poprawka 166
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 6 – ustęp 4 a (nowy)

Tekst proponowany przez Komisję

Poprawka

4a. Jeżeli przepisy Unii przewidują dla danego sektora unijny organ nadzorczy lub regulacyjny, między innymi w zakresie bezpieczeństwa sieci i systemów informatycznych, zgodnie z art. 14 ust. 2 organ ten otrzymuje zgłoszenia incydentów od zainteresowanych podmiotów gospodarczych z tego sektora oraz posiada uprawnienia w zakresie wdrażania i egzekwowania, o których mowa w art. 15. Ten organ unijny ściśle współpracuje w zakresie tych obowiązków z właściwymi organami i pojedynczym

punktem kontaktowym przyjmującego państwa członkowskiego. Pojedynczy punkt kontaktowy przyjmującego państwa członkowskiego reprezentuje organ unijny w odniesieniu do obowiązków wynikających z rozdziału III.

Or. en

Uzasadnienie

Niniejsza poprawka zastępuje poprawkę 37. Jej celem jest doprecyzowanie roli poszczególnych organów w celu zapobiegania powielaniu zgłoszeń adresowanych zarówno do właściwych organów, jak i do pojedynczych punktów kontaktowych. Biorąc pod uwagę, że w niektórych sektorach incydenty zgłaszane są już organom unijnym, należy unikać powielania tych zgłoszeń.

Poprawka 167 Konstantinos Poupakis

Wniosek dotyczący dyrektywy Artykuł 8 – ustęp 1

Tekst proponowany przez Komisję

1. ***Właściwe organy*** i Komisja ustanawiają sieć („sieć współpracy”) służącą do współpracy w zakresie ***przeciwdziałania zagrożeniom i incydentom dotyczącym*** sieci i systemów informatycznych.

Poprawka

1. ***Pojedyncze punkty kontaktowe*** i Komisja, ***a także na wniosek ENISA,*** ustanawiają sieć („sieć współpracy”) służącą do ***opracowywania narzędzi do procedur identyfikacji, analizy i reagowania w obszarach związanych z bezpieczeństwem i zagrożeniami lub incydentami dotyczącymi*** sieci i systemów informatycznych.

Or. el

Poprawka 168 Malcolm Harbour

Wniosek dotyczący dyrektywy Artykuł 8 – ustęp 2

Tekst proponowany przez Komisję

2. Sieć współpracy umożliwia stałą łączność między Komisją a **właściwymi organami**. Na żądanie Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA) wspiera sieć współpracy poprzez zapewnianie wiedzy specjalistycznej i doradztwa.

Poprawka

2. Sieć współpracy umożliwia stałą łączność między Komisją a **pojedynczymi punktami kontaktowymi**. Na żądanie Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA) wspiera sieć współpracy poprzez zapewnianie wiedzy specjalistycznej i doradztwa. **W stosownych przypadkach podmioty gospodarcze i dostawcy rozwiązań z zakresu bezpieczeństwa cybernetycznego mogą również zostać zaproszeni do uczestnictwa w działaniach sieci współpracy, o której mowa w ust. 3 lit. g), h) oraz i).**

Or. en

Uzasadnienie

Oprócz poprawek sprawozdawcy umożliwiających podmiotom gospodarczym branie udziału w sieci współpracy należy także uwzględnić możliwość udziału w niej dostawców rozwiązań z zakresu bezpieczeństwa cybernetycznego, co może stanowić znaczącą wartość dodaną, ponieważ organizacje te mogą dostarczyć informacji na temat zagrożeń cybernetycznych zgromadzonych na podstawie danych w bazach ich klientów, a także przedstawić ujednoczony przegląd wymogów, wyzwań i najlepszych praktyk stosowanych w szerokim spektrum grup konsumenckich.

Poprawka 169

Vicente Miguel Garcés Ramón

**Wniosek dotyczący dyrektywy
Artykuł 8 – ustęp 3 – litera c**

Tekst proponowany przez Komisję

c) regularnie publikują **na wspólnej stronie internetowej** niemające poufnego charakteru informacje na temat aktualnych wczesnych ostrzeżeń i skoordynowanych reakcji;

Poprawka

c) regularnie publikują niemające poufnego charakteru informacje na temat aktualnych wczesnych ostrzeżeń i skoordynowanych reakcji **w głównych przestrzeniach cyfrowych, w których podobnie jak na stronach internetowych możliwe jest wyszukiwanie informacji za**

Poprawka 170
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 8 – ustęp 3 – litera d

Tekst proponowany przez Komisję

d) wspólnie omawiają i oceniają, **na wniosek państwa członkowskiego lub Komisji**, jedną krajową strategię w zakresie bezpieczeństwa sieci i informacji, lub ich większą liczbę, lub jeden krajowy plan współpracy w zakresie bezpieczeństwa sieci i informacji, lub ich większą liczbę, o których mowa w art. 5, w zakresie niniejszej dyrektywy;

Poprawka

d) wspólnie omawiają i oceniają jedną krajową strategię w zakresie bezpieczeństwa sieci i informacji, lub ich większą liczbę, lub jeden krajowy plan współpracy w zakresie bezpieczeństwa sieci i informacji, lub ich większą liczbę, o których mowa w art. 5, w zakresie niniejszej dyrektywy;

Uzasadnienie

Możliwość występowania z indywidualnym wnioskiem przez państwa członkowskie lub Komisję byłaby rozwiązaniem zbyt daleko idącym i uderzałaby w założenia konstruktywnego funkcjonowania takiej sieci współpracy.

Poprawka 171
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 8 – ustęp 3 – litera e

Tekst proponowany przez Komisję

e) wspólnie omawiają i oceniają, **na wniosek państwa członkowskiego lub Komisji**, skuteczność CERT, zwłaszcza w przypadku gdy ćwiczenia w zakresie

Poprawka

e) wspólnie omawiają i oceniają skuteczność CERT, zwłaszcza w przypadku gdy ćwiczenia w zakresie bezpieczeństwa sieci i informacji

bezpieczeństwa sieci i informacji
przeprowadzane są na poziomie unijnym;

przeprowadzane są na poziomie unijnym;

Or. en

Uzasadnienie

Możliwość występowania z indywidualnym wnioskiem przez państwa członkowskie lub Komisję byłaby rozwiązaniem zbyt daleko idącym i uderzałaby w założenia konstruktywnego funkcjonowania takiej sieci współpracy.

Poprawka 172 **Andreas Schwab**

Wniosek dotyczący dyrektywy **Artykuł 8 – ustęp 3 – litera f**

Tekst proponowany przez Komisję

f) współpracują i wymieniają się **informacjami dotyczącymi wszystkich istotnych kwestii z działającym przy Europolu Europejskim Centrum ds. Walki z Cyberprzestępczością oraz z innymi właściwymi organami europejskimi**, w szczególności w dziedzinach ochrony danych, energetyki, transportu, bankowości, **obrotu papierami wartościowymi** i opieki zdrowotnej;

Poprawka

f) współpracują i wymieniają się **wiedzą specjalistyczną na temat** istotnych kwestii **z zakresu bezpieczeństwa sieci i informacji**, w szczególności w dziedzinach ochrony danych, energetyki, transportu, bankowości, **rynków finansowych** i opieki zdrowotnej **z działającym przy Europolu Europejskim Centrum ds. Walki z Cyberprzestępczością oraz z innymi właściwymi organami europejskimi**;

Or. en

Uzasadnienie

Niniejsza poprawka zastępuje poprawkę 44. Jej celem jest doprecyzowanie rodzaju informacji wymienianych z Europejskim Centrum ds. Walki z Cyberprzestępczością oraz z innymi właściwymi organami europejskimi.

Poprawka 173 **Andreas Schwab**

Wniosek dotyczący dyrektywy **Artykuł 8 – ustęp 3 – litera h**

Tekst proponowany przez Komisję

Poprawka

h) regularnie organizują wzajemne oceny zdolności i gotowości;

skreślona

Or. en

Uzasadnienie

Sprawozdawca popiera sieć współpracy; niemniej wzajemna ocena mogłaby stać w sprzeczności z istotnymi aspektami bezpieczeństwa narodowego, co nie byłoby objęte postanowieniami art. 114 TFUE.

Poprawka 174
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 8 – ustęp 3 – litera i a (nowa)

Tekst proponowany przez Komisję

Poprawka

ia) opracowują, we współpracy z ENISA, wytyczne dotyczące kryteriów dla danego sektora w odniesieniu do zgłaszania znaczących incydentów oprócz parametrów określonych w art. 14 ust. 2.

Or. en

Uzasadnienie

Niniejsza poprawka powinna znaleźć się po poprawce 45 (art. 6 ust. 3 ia (nowy)). Odesłanie do art. 14 ust. 2 powinno być czytane łącznie z poprawkami 56–59. Wprowadzie przedmiotowa dyrektywa przewiduje horyzontalne, międzysektorowe kryteria, których spełnienie pociąga za sobą konieczność dokonania zgłoszenia, ale niezbędne jest określenie osobnych kryteriów dla poszczególnych sektorów. W celu osiągnięcia ogólnounijnego stosowania przepisów dotyczących danego sektora, kryteria te powinny być opracowywane w ramach sieci i we współpracy z ENISA.

Poprawka 175
Philippe Juvin, Marielle Gallo

Wniosek dotyczący dyrektywy
Artykuł 8 – ustęp 3 a (nowy)

Tekst proponowany przez Komisję

Poprawka

3a. Właściwe organy przeprowadzają konsultacje z organami administracji publicznej i zainteresowanymi podmiotami gospodarczymi przed dokonaniem jakiegokolwiek wymiany, w ramach sieci współpracy, szczególnie chronionych i poufnych informacji dotyczących zagrożeń i incydentów mających wpływ na ich sieć i systemy informatyczne.

Or. en

Uzasadnienie

Celem niniejszej poprawki jest nadanie procedurze wymiany informacji w ramach sieci współpracy bardziej włączającego charakteru poprzez uwzględnienie potencjalnych komentarzy i uwag, które mogą zgłaszać organy administracji publicznej lub podmioty gospodarcze na temat szczególnie chronionych i poufnych informacji dotyczących zagrożeń i incydentów mających wpływ na ich sieć i systemy informatyczne. Właściwe organy mogą wziąć pod uwagę te uwagi, choć nie mają one wiążącego charakteru.

Poprawka 176
Christian Engström

Wniosek dotyczący dyrektywy
Artykuł 8 – ustęp 4

Tekst proponowany przez Komisję

Poprawka

4. Komisja ustanawia – w drodze aktów wykonawczych – niezbędne środki w celu ułatwienia współpracy pomiędzy właściwymi organami i Komisją, o której mowa w ust. 2 i 3. Te akty wykonawcze przyjmuje się zgodnie z procedurą **doradczą**, o której mowa w art. 19 ust. 2.

4. Komisja ustanawia – w drodze aktów wykonawczych – niezbędne środki w celu ułatwienia współpracy pomiędzy właściwymi organami i Komisją, o której mowa w ust. 2 i 3. Te akty wykonawcze przyjmuje się zgodnie z procedurą **sprawdzającą**, o której mowa w art. 19 ust. 2.

Or. en

Poprawka 177
Christian Engström

Wniosek dotyczący dyrektywy
Artykuł 9 – ustęp 1 a (nowy)

Tekst proponowany przez Komisję

Poprawka

1a. Dane osobowe są ujawniane tylko odbiorcom, którzy muszą przetwarzać je w ramach wykonywania swoich zadań zgodnie z odpowiednią podstawą prawną. Zakres ujawnianych danych ogranicza się do tego, co niezbędne do wykonywania tych zadań. Zapewnia się zgodność z zasadą celowości. Określa się termin przechowywania tych danych do celów wskazanych w niniejszej dyrektywie.

Or. en

Poprawka 178
Christian Engström

Wniosek dotyczący dyrektywy
Artykuł 9 – ustęp 1 b (nowy)

Tekst proponowany przez Komisję

Poprawka

1b. Kryteria udziału państw członkowskich w bezpiecznym systemie wymiany informacji zapewniają wysoki poziom bezpieczeństwa i odporności gwarantowane przez wszystkich uczestników na wszystkich etapach przetwarzania, w tym przez odpowiednie środki dotyczące poufności i bezpieczeństwa zgodnie z art. 16 i 17 dyrektywy 95/46/WE i art. 21 i 22 rozporządzenia (WE) nr 45/2001.

Or. en

Poprawka 179
Andreas Schwab, Malcolm Harbour

Wniosek dotyczący dyrektywy
Artykuł 9 – ustęp 2

Tekst proponowany przez Komisję

Poprawka

2. Komisja jest uprawniona do przyjęcia aktów delegowanych zgodnie z art. 18 dotyczących określenia kryteriów, jakie państwo członkowskie musi spełnić, aby móc uczestniczyć w bezpiecznym systemie wymiany informacji, w odniesieniu do:

skreślony

a) dostępności bezpiecznej i odpornej infrastruktury komunikacyjnej i informacyjnej na poziomie krajowym, kompatybilnej i interoperacyjnej z bezpieczną infrastrukturą sieci współpracy, zgodnie z art. 7 ust. 3, oraz

b) zapewnienia właściwemu organowi i CERT odpowiednich zasobów i procedur technicznych i finansowych oraz zasobów ludzkich w celu umożliwienia im skutecznego, efektywnego i bezpiecznego uczestnictwa w bezpiecznym systemie wymiany informacji zgodnie z art. 6 ust. 3, art. 7 ust. 2 i art. 7 ust. 3.

Or. en

Uzasadnienie

Niniejsza poprawka zastępuje poprawkę 47.

Poprawka 180
Christian Engström

Wniosek dotyczący dyrektywy
Artykuł 9 – ustęp 2 – wprowadzenie

Tekst proponowany przez Komisję

Poprawka

2. Komisja jest uprawniona do przyjęcia aktów delegowanych zgodnie z art. 18

(Nie dotyczy polskiej wersji językowej.)

dotyczących określenia kryteriów, jakie państwo członkowskie musi spełnić, aby móc uczestniczyć w bezpiecznym systemie wymiany informacji, w odniesieniu do:

Or. en

Poprawka 181
Andreas Schwab, Malcolm Harbour

Wniosek dotyczący dyrektywy
Artykuł 9 – ustęp 3

Tekst proponowany przez Komisję

3. Komisja przyjmuje – w drodze aktów wykonawczych – ***decyzje dotyczące dostępu państw członkowskich do tej bezpiecznej infrastruktury, zgodnie z kryteriami, o których mowa w ust. 2 i 3.*** Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 19 ust. 3.

Poprawka

3. Komisja przyjmuje – w drodze aktów wykonawczych – ***wspólny zestaw norm w zakresie wzajemnych połączeń i bezpieczeństwa, których pojedyncze punkty kontaktowe muszą przestrzegać przed wymianą szczególnie chronionych i poufnych informacji w ramach sieci współpracy.*** Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 19 ust. 3.

Or. en

Uzasadnienie

Należy opracować wspólny zestaw norm w zakresie wzajemnych połączeń i bezpieczeństwa w celu ochrony informacji i zapewnienia przejrzystości procesu oraz wymiany informacji na większą skalę między państwami członkowskimi w oparciu o wzajemne zaufanie.

Poprawka 182
Konstantinos Poupakis

Wniosek dotyczący dyrektywy
Artykuł 10 – ustęp 1 – wprowadzenie

Tekst proponowany przez Komisję

1. W ramach sieci współpracy **właściwe organy lub** Komisja wydają wczesne ostrzeżenia dotyczące zagrożeń i incydentów, które spełniają co najmniej jeden z następujących warunków:

Poprawka

1. W ramach sieci współpracy **pojedyncze punkty kontaktowe**, Komisja **lub ENISA** wydają wczesne ostrzeżenia dotyczące zagrożeń i incydentów, które spełniają co najmniej jeden z następujących warunków:

Or. el

Poprawka 183
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 10 – ustęp 1 – litera a

Tekst proponowany przez Komisję

a) ich skala szybko rośnie lub może szybko wzrosnąć;

Poprawka

skreślona

Or. en

Uzasadnienie

Kryterium to byłoby nieustannie spełnione i pociągałoby za sobą nieproporcjonalną liczbę wczesnych ostrzeżeń, które przekraczają zdolności odpowiedzialnych za nie organów. Ponadto rosnąca skala zagrożeń lub incydentów sama w sobie nie wymaga koniecznie podejmowania działań na szczeblu unijnym.

Poprawka 184
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 10 – ustęp 1 – litera b

Tekst proponowany przez Komisję

b) przekraczają one lub mogą przekroczyć krajowe zdolności reagowania;

Poprawka

b) w ocenie pojedynczego punktu kontaktowego dane zagrożenie lub incydent potencjalnie przekracza krajowe zdolności reagowania;

Uzasadnienie

Celem niniejszej poprawki jest dalsze doprecyzowanie kryteriów, których przestrzeganie pociąga za sobą wydanie wczesnych ostrzeżeń. Dalsze doprecyzowania powinny zostać wprowadzone w drodze aktów delegowanych w celu zapewnienia neutralności technicznej i uwzględnienia charakterystycznych warunków danego sektora.

Poprawka 185
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 10 – ustęp 1 – litera c

Tekst proponowany przez Komisję

c) mają *one wpływ lub mogą mieć* wpływ na więcej niż jedno państwo członkowskie.

Poprawka

c) *w ocenie pojedynczego punktu kontaktowego lub Komisji dane zagrożenie lub incydent ma* wpływ na więcej niż jedno państwo członkowskie.

Uzasadnienie

Celem niniejszej poprawki jest dalsze doprecyzowanie kryteriów, których przestrzeganie pociąga za sobą wydanie wczesnych ostrzeżeń. Dalsze doprecyzowania powinny zostać wprowadzone w drodze aktów delegowanych w celu zapewnienia neutralności technicznej i uwzględnienia charakterystycznych warunków danego sektora.

Poprawka 186
Catherine Stihler

Wniosek dotyczący dyrektywy
Artykuł 10 – ustęp 1 a (nowy)

Tekst proponowany przez Komisję

Poprawka

1a. Członkowie sieci współpracy podają do wiadomości publicznej uzyskane informacje dotyczące zagrożeń lub incydentów wyłącznie po otrzymaniu

*zgody od dokonującego zgłoszenia
właściwego organu krajowego.*

Or. en

Poprawka 187
Konstantinos Poupakis

Wniosek dotyczący dyrektywy
Artykuł 10 – ustęp 2 – akapit pierwszy a (nowy)

Tekst proponowany przez Komisję

Poprawka

***ENISA we współpracy z Komisją
opracowuje i obsługuje ogólnoeuropejski
mechanizm wczesnego ostrzegania i
reagowania jako uzupełnienie
mechanizmów funkcjonujących w
państwach członkowskich.***

Or. el

Poprawka 188
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 10 – ustęp 3

Tekst proponowany przez Komisję

Poprawka

***3. Na wniosek państwa członkowskiego
lub z własnej inicjatywy Komisja może
zwrócić się do państwa członkowskiego o
przedstawienie istotnych informacji
dotyczących określonego zagrożenia lub
incydentu.***

skreślony

Or. en

Uzasadnienie

W ust. 1 niniejszego artykułu określone są już warunki wydawania wczesnych ostrzeżeń. W związku z tym możliwość, by Komisja lub poszczególne państwa członkowskie zwracały się z

innymi bliżej nieokreślonymi wnioskami, byłaby rozwiązaniem zbyt daleko idącym i przynoszącym szkodę konstruktywnej współpracy.

Poprawka 189
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 10 – ustęp 4

Tekst proponowany przez Komisję

4. W sytuacji gdy zachodzi podejrzenie, iż zagrożenie lub incydent będące przedmiotem wczesnego ostrzeżenia **mają charakter przestępczy, właściwe organy lub Komisja powiadamiają** działające przy Europolu Europejskie Centrum ds. Walki z Cyberprzestępczością.

Poprawka

4. W sytuacji gdy zachodzi podejrzenie, iż zagrożenie lub incydent będące przedmiotem wczesnego ostrzeżenia **noszą znamiona poważnego przestępstwa, oraz jeżeli odnośny podmiot gospodarczy zgłosił incydenty noszące znamiona poważnego przestępstwa, zgodnie z art. 15 ust. 4, państwa członkowskie zapewniają, że – w stosownych przypadkach – zostanie o tym poinformowane** działające przy Europolu Europejskie Centrum ds. Walki z Cyberprzestępczością.

Or. en

Uzasadnienie

Niniejsza poprawka zastępuje poprawkę 50. Zgodnie z zasadą legalności organy inne niż organy ścigania nie mogą być zobowiązane do przestrzegania tej zasady i automatycznego powiadamiania o incydentach mających charakter przestępczy. Kontakty między organami niebędącymi organami ścigania a Europejskim Centrum ds. Walki z Cyberprzestępczością nie mogą być regulowane przepisami niniejszej dyrektywy.

Poprawka 190
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 10 – ustęp 4 a (nowy)

Tekst proponowany przez Komisję

Poprawka

4a. Członkowie sieci współpracy nie podają do wiadomości publicznej żadnych

otrzymanych informacji na temat zagrożeń i incydentów zgodnie z ust. 1 bez otrzymania uprzednio zgody pojedynczego punktu kontaktowego dokonującego zgłoszenia.

Or. en

Uzasadnienie

Celem niniejszej poprawki jest utrzymanie zaufania oraz zachęcenie do wymiany informacji poprzez koordynację publikacji wczesnych ostrzeżeń.

**Poprawka 191
Malcolm Harbour**

**Wniosek dotyczący dyrektywy
Artykuł 10 – ustęp 4 a (nowy)**

Tekst proponowany przez Komisję

Poprawka

4a. Członkowie sieci współpracy, a także Komisja nie podają do wiadomości publicznej żadnych otrzymanych informacji na temat zagrożeń lub incydentów zgodnie z ust. 1 bez otrzymania uprzednio zgody pojedynczego punktu kontaktowego dokonującego zgłoszenia; ponadto przed wymianą informacji w ramach sieci współpracy dokonujący zgłoszenia pojedynczy punkt kontaktowy informuje o swoim zamiarze podmiot gospodarczy, którego dane informacje dotyczą, i dokonuje ich anonimizacji, jeżeli podmiot gospodarczy uzna to za stosowne.

Or. en

Uzasadnienie

Zapis ten jest istotny z punktu widzenia budowania zaufania i zachęcania do wymiany informacji. Bez tych zabezpieczeń właściwe organy krajowe i podmioty gospodarcze z dużym prawdopodobieństwem wstrzymywałyby się od zgłaszania incydentów i od wymiany

informacji.

Poprawka 192
Christian Engström

Wniosek dotyczący dyrektywy
Artykuł 11 – ustęp 2 a (nowy)

Tekst proponowany przez Komisję

Poprawka

2a. W ramach planu skoordynowanej reakcji uwzględnia się zapewnienie dostatecznych rezerw.

Or. en

Poprawka 193
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Artykuł 12 – tytuł

Tekst proponowany przez Komisję

Poprawka

Unijny plan współpracy w zakresie bezpieczeństwa sieci i informacji

Plan współpracy ***i europejska strategia*** w zakresie bezpieczeństwa sieci i informacji

Or. es

Poprawka 194
Christian Engström

Wniosek dotyczący dyrektywy
Artykuł 12 – ustęp 3 a (nowy)

Tekst proponowany przez Komisję

Poprawka

3a. Unijny plan współpracy w zakresie bezpieczeństwa sieci i informacji jest opracowywany w taki sposób, aby był spójny z krajowymi strategiami w zakresie bezpieczeństwa sieci i informacji oraz z

planami współpracy określonymi w art. 5 niniejszej dyrektywy, przy uwzględnieniu w stosownych przypadkach analizy, o której mowa w motywie 13a.

Or. en

Uzasadnienie

Zob. poprawkę zaproponowaną przez Christiana Engströma w odniesieniu do nowego motywu 13a.

Poprawka 195 **Sari Essayah**

Wniosek dotyczący dyrektywy **Artykuł 13**

Tekst proponowany przez Komisję

Bez uszczerbku dla możliwości podejmowania nieformalnej współpracy międzynarodowej przez sieć współpracy, Unia może zawierać umowy międzynarodowe z państwami trzecimi lub organizacjami międzynarodowymi, umożliwiając oraz organizując ich udział w określonych działaniach sieci współpracy. Takie umowy uwzględniają potrzebę zapewnienia odpowiedniej ochrony danych osobowych, które są przekazywane w ramach sieci współpracy.

Poprawka

Bez uszczerbku dla możliwości podejmowania nieformalnej współpracy międzynarodowej przez sieć współpracy, Unia może zawierać umowy międzynarodowe z państwami trzecimi lub organizacjami międzynarodowymi, umożliwiając oraz organizując ich udział w określonych działaniach sieci współpracy. Takie umowy uwzględniają potrzebę zapewnienia odpowiedniej ochrony danych osobowych, które są przekazywane w ramach sieci współpracy. ***Na szczelnu międzynarodowym celem Unii jest wywieranie wpływu na dostawców usług sieci społecznościowej, tak aby odszukiwanie odpowiednich ustawień dotyczących bezpieczeństwa nie było pozostawiane użytkownikowi, lecz aby automatycznie zapewnione były maksymalne bezpieczeństwo i szyfrowanie wiadomości i aby użytkownik dopiero później mógł świadomie zezwolić na mniej rygorystyczne ustawienia bezpieczeństwa dla konkretnych celów.***

Poprawka 196
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Artykuł 13

Tekst proponowany przez Komisję

Bez uszczerbku dla możliwości podejmowania nieformalnej współpracy międzynarodowej przez sieć współpracy, Unia może zawierać umowy międzynarodowe z państwami trzecimi lub organizacjami międzynarodowymi, umożliwiając oraz organizując ich udział w określonych działaniach sieci współpracy. Takie umowy uwzględniają potrzebę zapewnienia odpowiedniej ochrony danych osobowych, które są przekazywane w ramach sieci współpracy.

Poprawka

Bez uszczerbku dla możliwości podejmowania nieformalnej współpracy międzynarodowej przez sieć współpracy, Unia może zawierać umowy międzynarodowe z państwami trzecimi lub organizacjami międzynarodowymi, umożliwiając oraz organizując ich udział w określonych działaniach sieci współpracy. Takie umowy uwzględniają potrzebę zapewnienia odpowiedniej ochrony danych osobowych, które są przekazywane w ramach sieci współpracy. ***Umowy te powinny zarazem chronić suwerenność UE oraz niezależność jej instytucji i państw członkowskich.***

Or. es

Poprawka 197
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 13 a (nowy)

Tekst proponowany przez Komisję

Poprawka

Artykuł 13a

Poziom krytyczności podmiotów gospodarczych

Państwa członkowskie mogą określić poziom krytyczności podmiotów gospodarczych, biorąc pod uwagę specyfikę sektorów, parametry obejmujące

znaczenie konkretnego podmiotu gospodarczego dla utrzymania wystarczającego poziomu usług sektorowych, liczbę części dostarczanych przez dany podmiot gospodarczy oraz okres, po upływie którego brak ciągłości świadczenia usług podstawowych przez podmiot gospodarczy ma negatywny wpływ na utrzymanie kluczowych działań gospodarczych i społecznych.

Or. en

Uzasadnienie

Niniejsza poprawka stanowi część rozdziału IV i powinna w nim poprzedzać art. 14. Celem niniejszego artykułu jest umożliwienie bardziej zróżnicowanej klasyfikacji załącznika II oraz w konsekwencji – obowiązków określonych w rozdziale IV. Zgłaszanie incydentu powinno być dokonywane przez wszystkie podmioty gospodarcze niezależnie od ich poziomu krytyczności, podczas gdy forma audytów bezpieczeństwa może zostać dostosowana do konkretnego poziomu krytyczności danego podmiotu gospodarczego.

Poprawka 198 Andreas Schwab

Wniosek dotyczący dyrektywy Rozdział IV – tytuł

Tekst proponowany przez Komisję

**BEZPIECZEŃSTWO SIECI I
SYSTEMÓW INFORMATYCZNYCH
ORGANÓW ADMINISTRACJI
PUBLICZNEJ I PODMIOTÓW
GOSPODARCZYCH**

Poprawka

**BEZPIECZEŃSTWO SIECI I
SYSTEMÓW INFORMATYCZNYCH
PODMIOTÓW GOSPODARCZYCH**

Or. en

Uzasadnienie

Dostosowanie zgodnie z projektem sprawozdania.

Poprawka 199
Christian Engström

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 1

Tekst proponowany przez Komisję

1. Państwa członkowskie zapewniają zastosowanie przez organy administracji publicznej i podmioty gospodarcze właściwych środków technicznych i organizacyjnych w celu przeciwdziałania zagrożeniom, na jakie narażone są kontrolowane i wykorzystywane przez nie sieci i systemy informatyczne.

Uwzględniając aktualny stan wiedzy i technologii, środki te zapewniają poziom bezpieczeństwa stosowny do istniejącego zagrożenia. W szczególności należy **podjąć** środki zapobiegające incydom dotyczącym sieci i systemów informatycznych organów administracji publicznej i podmiotów gospodarczych oraz minimalizujące wpływ tych incydentów na świadczone przez nie podstawowe usługi, zapewniając tym samym ciągłość usług opartych na tych sieciach i systemach informatycznych.

Poprawka

1. Państwa członkowskie zapewniają zastosowanie przez organy administracji publicznej i podmioty gospodarcze właściwych środków technicznych i organizacyjnych w celu przeciwdziałania zagrożeniom, na jakie narażone są kontrolowane i wykorzystywane przez nie sieci i systemy informatyczne. Środki te zapewniają poziom bezpieczeństwa stosowny do istniejącego zagrożenia, **a w szczególności należy przyjąć skuteczne i proporcjonalne** środki zapobiegające incydom dotyczącym sieci i systemów informatycznych organów administracji publicznej i podmiotów gospodarczych oraz minimalizujące wpływ tych incydentów na świadczone przez nie podstawowe usługi, zapewniając tym samym ciągłość usług **podstawowych** opartych na tych sieciach i systemach informatycznych. **W stosownych przypadkach organy administracji publicznej i podmioty gospodarcze muszą także przyjąć na własny koszt odpowiednie i natychmiastowe środki w celu zaradzenia wszelkim nowym, nieprzewidzianym zagrożeniom bezpieczeństwa oraz przywrócić normalny poziom bezpieczeństwa danej usługi.**

Or. en

Poprawka 200
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 1

Tekst proponowany przez Komisję

1. Państwa członkowskie zapewniają zastosowanie przez **organy administracji publicznej i** podmioty gospodarcze właściwych środków technicznych i organizacyjnych w celu przeciwdziałania zagrożeniom, na jakie narażone są kontrolowane i wykorzystywane przez nie sieci i systemy informatyczne. Uwzględniając aktualny stan wiedzy i technologii, środki te zapewniają poziom bezpieczeństwa stosowny do istniejącego zagrożenia. W szczególności należy podjąć środki zapobiegające incydom dotyczącym sieci i systemów informatycznych organów administracji publicznej i podmiotów gospodarczych oraz minimalizujące wpływ tych incydentów na świadczone przez nie podstawowe usługi, zapewniając tym samym ciągłość usług opartych na tych sieciach i systemach informatycznych.

Poprawka

1. Państwa członkowskie zapewniają zastosowanie przez podmioty gospodarcze właściwych **i proporcjonalnych** środków technicznych i organizacyjnych w celu przeciwdziałania zagrożeniom, na jakie narażone są kontrolowane i wykorzystywane przez nie sieci i systemy informatyczne. Uwzględniając aktualny stan wiedzy i technologii, środki te zapewniają poziom bezpieczeństwa stosowny do istniejącego zagrożenia. W szczególności należy podjąć środki zapobiegające incydom dotyczącym sieci i systemów informatycznych organów administracji publicznej i podmiotów gospodarczych oraz minimalizujące wpływ tych incydentów na świadczone przez nie podstawowe usługi, zapewniając tym samym ciągłość usług opartych na tych sieciach i systemach informatycznych.

Or. en

Uzasadnienie

Niniejsza poprawka zastępuje poprawkę 55.

Poprawka 201
Philippe Juvin, Marielle Gallo

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 2 – akapit pierwszy a (nowy)

Tekst proponowany przez Komisję

Poprawka

Operatorzy infrastruktury krytycznej, o których mowa w art. 3 ust. 8 lit. b), zgłaszają wyłącznie te incydenty – określone w poprzednich akapitach – które są bezpośrednio związane z ochroną infrastruktury krytycznej.

Uzasadnienie

Niniejsza poprawka odzwierciedla zmianę wprowadzoną w art. 3 ust. 8 lit. b) dotyczącą definicji drugiego rodzaju podmiotu gospodarczego (operatora infrastruktury krytycznej). Nie wszystkie sieci i systemy informatyczne należące do operatora infrastruktury krytycznej są bowiem „krytyczne” w sensie posiadania przez nie zasadniczego znaczenia dla utrzymania kluczowych działań. Zakresem stosowania niniejszej dyrektywy powinny być objęte wyłącznie te sieci i systemy informatyczne, które są bezpośrednio związane z infrastrukturą krytyczną.

Poprawka 202
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 2 – akapit pierwszy a (nowy)

Tekst proponowany przez Komisję

Poprawka

Parametry te zostają doprecyzowane zgodnie z art. 8 ust. 3 lit. ib).

Uzasadnienie

Niniejsza poprawka powinna znaleźć się po poprawkach 57, 58, 59 jako trzecie zdanie ust. 2. Poprawka odnosi się do nowej poprawki dotyczącej wytycznych zaproponowanych w art. 8 ust. 3.

Poprawka 203
Christian Engström

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 2 a (nowy)

Tekst proponowany przez Komisję

Poprawka

2a. Producenci oprogramowania są odpowiedzialni za przeprowadzenie działań zaradczych w przypadku naruszeń bezpieczeństwa, w ciągu 24 godzin od otrzymania informacji w poważnych

przypadkach i w ciągu 72 godzin w przypadkach, gdy mało prawdopodobne są skutki w postaci znacznych strat finansowych lub poważnego naruszenia prywatności.

Or. en

Poprawka 204
Philippe Juvín, Marielle Gallo

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 2 a (nowy)

Tekst proponowany przez Komisję

Poprawka

2a. Aby ocenić, czy dany incydent ma znaczące konsekwencje dla bezpieczeństwa usług podstawowych świadczonych przez organy administracji publicznej i podmioty gospodarcze, należy szczególnie wziąć pod uwagę następujące kryteria:

- a) liczbę użytkowników zależnych od danej usługi podstawowej, na których ten incydent ma wpływ;*
- b) skalę szkody wyrządzonej tym użytkownikom;*
- c) czas trwania incydentu;*
- d) gospodarcze i społeczne skutki incydentu;*
- e) ewentualny wpływ na dane osobowe użytkowników.*

Or. en

Uzasadnienie

Pojęcie „znaczących konsekwencji” musi zostać doprecyzowane w celu lepszego określania incydentów, które należy zgłaszać. Niniejszy wykaz ma charakter niewyczerpujący i można by uwzględnić także inne kryteria w zależności od specyfiki danego incydentu.

Poprawka 205
Christian Engström

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 2 b (nowy)

Tekst proponowany przez Komisję

Poprawka

2b. Klauzule o nieponoszeniu odpowiedzialności nie mogą chronić producentów oprogramowania komercyjnego, gdy można wykazać, że ich produkty nie zostały odpowiednio zaprojektowane na wypadek przewidywalnych zagrożeń bezpieczeństwa.

Or. en

Poprawka 206
Christian Engström

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 2 c (nowy)

Tekst proponowany przez Komisję

Poprawka

2c. Odnośny organ nadzorczy również informuje społeczeństwo lub nakłada taki obowiązek na dostawcę usług zaufania. Zgłoszenie i podanie informacji do wiadomości publicznej dokonuje się zwykle bez zbędnej zwłoki; dostawca usług zaufania może jednak zwrócić się o pozwolenie na późniejsze zgłoszenie i podanie informacji, tak aby można było usunąć problem związany z najbardziej wrażliwymi danymi. Jeśli organ nadzorczy udzieli zezwolenia na takie opóźnienie, nie może ono przekraczać terminu 45 dni, a podmiot odpowiedzialny musi zgodzić się na wypłatę odszkodowania wszystkim ufającym stronom, bez względu na ich lokalizację na świecie, w związku ze stratami wynikającymi bezpośrednio z opóźnienia w dokonaniu zgłoszenia.

Poprawka 207
Catherine Stihler

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 4

Tekst proponowany przez Komisję

4. W przypadku gdy właściwy organ uznaje, że ujawnienie incydentu leży w interesie publicznym, może on podać informację o incydencie do wiadomości publicznej lub zobowiązać do tego organy administracji publicznej lub podmioty gospodarcze. Raz do roku właściwy organ przekazuje sieci współpracy sprawozdanie podsumowujące otrzymane zgłoszenia i działania podjęte zgodnie z niniejszym ustępem.

Poprawka

4. W przypadku gdy właściwy organ uznaje, że ujawnienie incydentu leży w interesie publicznym, może on podać informację o incydencie do wiadomości publicznej lub zobowiązać do tego organy administracji publicznej lub podmioty gospodarcze. Raz do roku właściwy organ przekazuje sieci współpracy sprawozdanie podsumowujące otrzymane zgłoszenia i działania podjęte zgodnie z niniejszym ustępem. ***W przypadku incydentów zgłoszonych w ramach sieci współpracy, o której mowa w art. 8, inne właściwe organy krajowe podają do wiadomości publicznej wszelkie uzyskane informacje dotyczące zagrożeń lub incydentów wyłącznie po otrzymaniu zgody od dokonującego zgłoszenia właściwego organu krajowego.***

Poprawka 208
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 4

Tekst proponowany przez Komisję

4. W przypadku gdy właściwy organ uznaje, że ujawnienie incydentu leży w interesie publicznym, może on podać informację o incydencie do wiadomości

Poprawka

4. W przypadku gdy właściwy organ uznaje, że ujawnienie incydentu leży w interesie publicznym, może on podać informację o incydencie do wiadomości

publicznej lub zobowiązać do tego organy administracji publicznej lub podmioty gospodarcze. Raz do roku właściwy organ przekazuje sieci współpracy sprawozdanie podsumowujące otrzymane zgłoszenia i działania podjęte zgodnie z niniejszym ustępem.

publicznej lub zobowiązać do tego organy administracji publicznej lub podmioty gospodarcze. Raz do roku właściwy organ przekazuje sieci współpracy sprawozdanie podsumowujące otrzymane zgłoszenia i działania podjęte zgodnie z niniejszym ustępem. ***W tym sprawozdaniu rocznym musi być podana przynajmniej liczba wydanych zgłoszeń oraz podział zgłoszeń ze względu na ich charakter.***

Sprawozdanie udostępniane jest obywatelom w kompatybilnym formacie umożliwiającym jego publikację na wszelkich portalach otwartych danych, które zechcą opublikować jego treść.

Or. es

Poprawka 209 Andreas Schwab

Wniosek dotyczący dyrektywy Artykuł 14 – ustęp 4

Tekst proponowany przez Komisję

4. W przypadku gdy właściwy organ uznaje, że ujawnienie incydentu leży w interesie publicznym, może on podać informację o incydencie do wiadomości publicznej lub zobowiązać do tego organy administracji publicznej lub podmioty gospodarcze. Raz do roku właściwy organ przekazuje sieci współpracy sprawozdanie podsumowujące otrzymane zgłoszenia i działania podjęte zgodnie z niniejszym ustępem.

Poprawka

4. Po konsultacji z powiadomionym właściwym organem i zainteresowanym podmiotem gospodarczym pojedynczy punkt kontaktowy może poinformować opinię publiczną o poszczególnych incydentach, jeżeli wiedza obywateli na ten temat jest niezbędna, by zapobiec incydentowi bądź uporać się z bieżącym incydemem, lub jeżeli podmiot gospodarczy, którego dotyczy dany incydent, odmówił niezwłocznego usunięcia poważnej strukturalnej usterki związanej z tym incydemem. Przed jakimkolwiek publicznym ujawnieniem informacji powiadomiony właściwy organ zapewnia zainteresowanemu podmiotowi gospodarczemu możliwość bycia wysłuchanym.

Raz do roku ***pojedynczy punkt kontaktowy***

przekazuje sieci współpracy sprawozdanie podsumowujące otrzymane zgłoszenia i działania podjęte zgodnie z niniejszym ustępem.

Or. en

Uzasadnienie

Niniejsza poprawka zastępuje poprawkę 61 projektu sprawozdania, a jej celem jest zapewnienie wzmocnienia prawa podmiotów gospodarczych do bycia wysłuchanymi przed ujawnieniem poszczególnych incydentów. Umożliwia ona ponadto pojedynczemu punktowi kontaktowemu weryfikację i uzupełnienie informacji, które mają zostać ujawnione.

Poprawka 210 Malcolm Harbour

Wniosek dotyczący dyrektywy Artykuł 14 – ustęp 4 a (nowy)

Tekst proponowany przez Komisję

Poprawka

4a. Właściwy organ zapewnia, że wszystkie informacje, które otrzymał w ramach obowiązku zgłaszania incydentów, zostały poddane anonimizacji w każdym przypadku, gdy informacje takie zostają przekazane stronom trzecim.

Or. en

Uzasadnienie

Jest to mający zasadnicze znaczenie środek na rzecz budowania zaufania i zachęcania do wymiany informacji. Bez takiego zabezpieczenia właściwe organy krajowe, a co za tym idzie także podmioty gospodarcze, z niechęcią odnosiłyby się do zgłaszania incydentów i wymiany informacji.

Poprawka 211 Toine Manders

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 4 a (nowy)

Tekst proponowany przez Komisję

Poprawka

4a. Każdego roku państwa członkowskie przedstawiają Komisji i sieci współpracy wykaz organów administracji publicznej i podmiotów gospodarczych, które nie wskazują incydentów prawidłowo. Wykaz taki może zostać udostępniony publicznie.

Or. en

Poprawka 212
Malcolm Harbour

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 6 a (nowy)

Tekst proponowany przez Komisję

Poprawka

6a. Właściwe organy lub pojedyncze punkty kontaktowe sporządzają plan, w którym wyraźnie określa się cel zgłaszania incydentów, sposób wykorzystania zgłoszonych informacji oraz formaty i procedury wymagane przy wdrażaniu przepisów ust. 2, zwłaszcza w odniesieniu do poufności i anonimowości informacji.

Or. en

Uzasadnienie

Informacje dotyczące incydentu mogą wymagać wyjątkowej ochrony, zwłaszcza w związku z tym, że wykrywanie może skłonić wrogi podmiot do zmiany zachowania lub zacierania śladów. Zgłoszenie incydentu może również spowodować utratę reputacji, jeśli informacje na temat incydentu zostaną ujawnione publicznie. Dlatego też proces zgłaszania i treść zgłoszeń powinny być związane z ostatecznym wykorzystaniem uzyskanych informacji, tak aby zachęcać do terminowego i pełnego zgłaszania, a zasadnicze znaczenie powinno mieć wdrożenie odpowiednich kontroli w zakresie bezpieczeństwa, w tym w odniesieniu do anonimizacji informacji.

Poprawka 213
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 8 a (nowy)

Tekst proponowany przez Komisję

Poprawka

8a. Państwa członkowskie mogą podjąć decyzję o stosowaniu do organów administracji publicznej odpowiednio niniejszego artykułu i art. 15.

Or. en

Uzasadnienie

Informacje dotyczące incydentu mogą wymagać wyjątkowej ochrony, zwłaszcza w związku z tym, że wykrywanie może skłonić wrogi podmiot do zmiany zachowania lub zacierania śladów. Zgłoszenie incydentu może również spowodować utratę reputacji, jeśli informacje na temat incydentu zostaną ujawnione publicznie. Dlatego też proces zgłaszania i treść zgłoszeń powinny być związane z ostatecznym wykorzystaniem uzyskanych informacji, tak aby zachęcać do terminowego i pełnego zgłaszania, a zasadnicze znaczenie powinno mieć wdrożenie odpowiednich kontroli w zakresie bezpieczeństwa, w tym w odniesieniu do anonimizacji informacji.

Poprawka 214
Toine Manders

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 1 a (nowy)

Tekst proponowany przez Komisję

Poprawka

1a. Państwa członkowskie zapewniają właściwym organom uprawnienia w zakresie dokonywania oceny prawidłowości dowodów i zgłaszania incydentów przez organy administracji publicznej lub podmioty gospodarcze.

Or. en

Poprawka 215
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 2 – litera b

Tekst proponowany przez Komisję

b) *poddania się audytowi* bezpieczeństwa *przeprowadzonemu* przez wykwalifikowany niezależny podmiot lub organ krajowy oraz udostępnienia *wyników tego audytu* właściwemu organowi.

Poprawka

b) *dostarczenia dowodów skutecznej realizacji polityki w zakresie bezpieczeństwa, takich jak wyniki audytu* bezpieczeństwa *przeprowadzonego* przez wykwalifikowany niezależny podmiot lub organ krajowy, oraz udostępnienia *tych dowodów* właściwemu organowi *lub pojedynczemu punktowi kontaktowemu*.

Or. en

Uzasadnienie

Niniejsza poprawka zastępuje poprawkę 66, a jej celem jest ustanowienie zróżnicowanych wymogów w zakresie audytu przy uwzględnieniu specyfiki danego podmiotu gospodarczego.

Poprawka 216
Toine Manders

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 2 – litera b a (nowa)

Tekst proponowany przez Komisję

Poprawka

ba) zachęcanie państw członkowskich do zmniejszenia liczby i intensywności audytów w odniesieniu do tego podmiotu gospodarczego lub organu administracji publicznej, jeśli przeprowadzony w nim audyt bezpieczeństwa wykazuje w spójny sposób dobre wyniki.

Or. en

Poprawka 217
Toine Manders

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 3 a (nowy)

Tekst proponowany przez Komisję

Poprawka

3a. Państwa członkowskie zapewniają, że właściwe organy poddawają się co roku audytowi bezpieczeństwa. Wyniki tych audytów podaje się do wiadomości publicznej.

Or. en

Poprawka 218
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 3 a (nowy)

Tekst proponowany przez Komisję

Poprawka

3a. W drodze odstępstwa od ust. 2 lit. b) niniejszego artykułu państwa członkowskie mogą zdecydować, że właściwe organy lub pojedyncze punkty kontaktowe, w zależności od wymogów, mają stosować inną procedurę w odniesieniu do konkretnych podmiotów gospodarczych w oparciu o ich poziom krytyczności określony zgodnie z art. 13a. W przypadku gdy państwa członkowskie podejmą taką decyzję:

a) właściwe organy lub pojedyncze punkty kontaktowe, w zależności od wymogów, są uprawnione do wystąpienia z wystarczająco konkretnym wnioskiem do podmiotów gospodarczych zobowiązującym je do dostarczenia dowodów skutecznej realizacji polityki w zakresie bezpieczeństwa, takich jak wyniki audytu bezpieczeństwa przeprowadzonego przez wykwalifikowanego audytora wewnętrznego, oraz udostępnienia tych

dowodów właściwemu organowi lub pojedynczemu punktowi kontaktowemu;
b) w stosownych przypadkach właściwy organ lub pojedynczy punkt kontaktowy mogą – po przedłożeniu przez podmiot gospodarczy dokumentów, o których mowa w lit. a) – zażądać dodatkowych dowodów lub przeprowadzenia dodatkowego audytu przez wykwalifikowany niezależny podmiot lub organ krajowy.

Or. en

Poprawka 219
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 4

Tekst proponowany przez Komisję

4. Właściwe organy **zgłaszają** organom ścigania **poważne incydenty, które mogą mieć charakter przestępczy.**

Poprawka

4. Właściwe organy **i pojedyncze punkty kontaktowe informują zainteresowane podmioty gospodarcze o możliwości zgłaszania** organom ścigania **incydentów noszących znamiona poważnego przestępstwa.**

Or. en

Uzasadnienie

Niniejsza poprawka zastępuje poprawkę 69. Należy pozostawić zainteresowanemu podmiotowi gospodarczemu swobodę w zakresie wyboru, czy wystąpić z oskarżeniem w związku z incydentami noszącymi znamiona poważnego przestępstwa. Zgodnie z zasadą legalności organy inne niż organy ścigania nie mogą być zobowiązane do przestrzegania tej zasady i automatycznego powiadamiania o incydentach noszących znamiona przestępstwa.

Poprawka 220
Sylvana Rapti

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 5

Tekst proponowany przez Komisję

5. W przypadku incydentów prowadzących do naruszeń danych osobowych właściwe organy działają w ścisłej współpracy z organami ochrony danych **osobowych**.

Poprawka

5. W przypadku incydentów prowadzących do naruszeń danych osobowych właściwe organy ***i pojedyncze punkty kontaktowe*** działają w ścisłej współpracy z organami ochrony danych. ***Pojedyncze punkty kontaktowe i organy ochrony danych opracowują, w ramach współpracy z ENISA, mechanizmy wymiany informacji oraz pojedynczy wzór formularza wykorzystywanego zarówno w przypadku zgłoszeń na podstawie art. 14 ust. 2 niniejszej dyrektywy, jak i na podstawie dyrektywy 95/46/WE Parlamentu Europejskiego i Rady¹.***

¹***Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. L 281 z 23.11.1995, s. 31).***

Or. en

Poprawka 221
Konstantinos Poupakis

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 5

Tekst proponowany przez Komisję

5. W przypadku incydentów prowadzących do naruszeń danych osobowych właściwe organy działają w ścisłej współpracy z organami ochrony danych osobowych.

Poprawka

5. W przypadku incydentów prowadzących do naruszeń danych osobowych właściwe organy ***i pojedyncze punkty kontaktowe*** działają w ścisłej współpracy z organami ochrony danych osobowych. ***Pojedyncze punkty kontaktowe i organy ochrony danych osobowych opracowują we współpracy z ENISA mechanizmy***

wymiany informacji i jednolity wzór formularza stosowany zarówno w odniesieniu do zgłoszeń, o których mowa w art. 14 ust. 2 niniejszej dyrektywy, jak i w rozporządzeniu (xxx) Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje i organy wspólnotowe oraz swobodnego przepływu takich danych.

Or. el

Poprawka 222
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 6 a (nowy)

Tekst proponowany przez Komisję

Poprawka

6a. Państwa członkowskie mogą podjąć decyzję o stosowaniu odpowiednio art. 14 i niniejszego artykułu do organów administracji publicznej.

Or. en

Poprawka 223
Toine Manders

Wniosek dotyczący dyrektywy
Artykuł 16 – ustęp 1

Tekst proponowany przez Komisję

Poprawka

1. W celu zapewnienia spójnego wdrażania art. 14 ust. 1 państwa członkowskie wspierają stosowanie norm lub specyfikacji mających znaczenie dla bezpieczeństwa sieci i informacji.

1. W celu zapewnienia spójnego wdrażania art. 14 ust. 1 państwa członkowskie wspierają stosowanie ***międzynarodowych lub europejskich*** norm lub specyfikacji mających znaczenie dla bezpieczeństwa sieci i informacji. ***Podmiotom gospodarczym pozostawia się swobodę w zakresie stosowania dodatkowych środków mających na celu osiągnięcie wyższego***

poziomu bezpieczeństwa.

Or. en

Poprawka 224
Christian Engström

Wniosek dotyczący dyrektywy
Artykuł 16 – ustęp 1

Tekst proponowany przez Komisję

1. W celu zapewnienia spójnego wdrażania art. 14 ust. 1 państwa członkowskie wspierają stosowanie norm lub specyfikacji mających znaczenie dla bezpieczeństwa sieci i informacji.

Poprawka

1. W celu zapewnienia spójnego wdrażania art. 14 ust. 1 państwa członkowskie wspierają stosowanie **otwartych** norm lub specyfikacji mających znaczenie dla bezpieczeństwa sieci i informacji.

Or. en

Poprawka 225
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 17 – ustęp 1 a (nowy)

Tekst proponowany przez Komisję

Poprawka

1a. Państwa członkowskie zapewniają, że sankcje, o których mowa w ust. 1 niniejszego artykułu, mają zastosowanie wyłącznie w przypadku, gdy podmiot gospodarczy celowo lub w wyniku rażącego zaniedbania nie wywiązał się z obowiązków przewidzianych w rozdziale IV.

Or. en

Uzasadnienie

Niniejsza poprawka zastępuje poprawkę 73, a jej brzmienie jest uproszczoną wersją pierwotnej poprawki.

Poprawka 226
Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy
Artykuł 17 – ustęp 2 a (nowy)

Tekst proponowany przez Komisję

Poprawka

2a. Właściwe organy pociągają do odpowiedzialności dostawców wadliwego komputerowego oprogramowania, sprzętu lub usług przyczyniających się w sposób bezpośredni do powstawania incydentów w zakresie bezpieczeństwa sieci i informacji.

Or. es

Poprawka 227
Andreas Schwab

Wniosek dotyczący dyrektywy
Artykuł 18 – ustęp 2

Tekst proponowany przez Komisję

Poprawka

2. Uprawnienia do przyjęcia aktów delegowanych, o których mowa w **art. 9 ust. 2**, art. 10 ust. 5 **i art. 14 ust. 5**, powierza się Komisji. Komisja sporządza sprawozdanie dotyczące przekazania uprawnień nie później niż dziewięć miesięcy przed końcem okresu wynoszącego pięć lat. Przekazanie uprawnień zostaje automatycznie przedłużone na takie same okresy, chyba że Parlament Europejski lub Rada sprzeciwią się takiemu przedłużeniu nie później niż trzy miesiące przed końcem każdego okresu.

2. Uprawnienia do przyjęcia aktów delegowanych, o których mowa w art. 10 ust. 5, powierza się Komisji ***na okres pięciu lat od daty transpozycji, o której mowa w art. 21***. Komisja sporządza sprawozdanie dotyczące przekazania uprawnień nie później niż dziewięć miesięcy przed końcem okresu wynoszącego pięć lat. Przekazanie uprawnień zostaje automatycznie przedłużone na takie same okresy, chyba że Parlament Europejski lub Rada sprzeciwią się takiemu przedłużeniu nie później niż trzy miesiące przed końcem każdego okresu.

Or. en

Uzasadnienie

Sprawozdawca wycofuje poprawkę 47 i zastępuje ją poprawką polegającą na skreśleniu art. 9 ust. 2. Wycofuje on także poprawkę 51 i chciałby zachować ten akt delegowany w art. 10 ust. 5, biorąc pod uwagę, że kryteria zobowiązujące do wydawania wczesnych ostrzeżeń określone w art. 10 ust. 1 wymagają doprecyzowania w drodze aktów delegowanych, aby były neutralne technicznie i uwzględniały warunki konkretnego sektora itp. W celu uwzględnienia tych zmian dotyczących aktów delegowanych niniejsza poprawka zastępuje także poprawkę 74.

Poprawka 228

Vicente Miguel Garcés Ramón

Wniosek dotyczący dyrektywy

Załącznik II – akapit pierwszy – punkt 6 a (nowy)

Tekst proponowany przez Komisję

Poprawka

***6a. usługi w zakresie komunikatów na
rozmaitych platformach***

Or. es

Poprawka 229

Sari Essayah

Wniosek dotyczący dyrektywy

Załącznik II – akapit pierwszy – punkt 6 a (nowy)

Tekst proponowany przez Komisję

Poprawka

6a. serwery lustrzane

Or. en

Poprawka 230

Andreas Schwab

Wniosek dotyczący dyrektywy

Załącznik II – akapit pierwszy – punkt 2 – tiret pierwsze a (nowe)

Tekst proponowany przez Komisję

Poprawka

d) Transport morski

(i) przewoźnicy morscy (przedsiębiorstwa świadczące usługi pasażerskiego transportu śródlądowego, morskiego i przybrzeżnego oraz przedsiębiorstwa świadczące usługi towarowego transportu śródlądowego, morskiego i przybrzeżnego)

(ii) porty

(iii) operatorzy zarządzający ruchem

(iv) pomocnicze usługi logistyczne:

– magazynowanie i składowanie

– przeladunek oraz

– pozostała działalność wspomagająca transport

Or. en

Uzasadnienie

Niniejsza poprawka zastępuje poprawkę 97 projektu sprawozdania, a jej celem jest uwzględnienie również żeglugi śródlądowej.

Poprawka 231
Andreas Schwab

Wniosek dotyczący dyrektywy
Załącznik II – akapit pierwszy – punkt 2 a (nowy)

Tekst proponowany przez Komisję

Poprawka

2a. Usługi wodne

Or. en

Uzasadnienie

Usługi wodne, określone w art. 2 pkt 38 dyrektywy 2000/60/WE, a zwłaszcza większe obszary świadczenia takich usług obsługiwane są w dużej mierze przez systemy informatyczne, w tym w zakresie składu wody przeznaczonej do spożycia przez ludzi. Ponadto w przypadku niektórych większych obszarów awaria systemów informatycznych mogłaby nieść z sobą ryzyko podniesienia się poziomu wód gruntowych z potencjalnymi skutkami o charakterze krytycznym, tj. z przerwaniem tam. W związku z tym usługi wodne powinny zostać uwzględnione w załączniku II.

Poprawka 232
Malcolm Harbour

Wniosek dotyczący dyrektywy
Załącznik II – akapit pierwszy – punkt 5

Tekst proponowany przez Komisję

5. Służba zdrowia: punkty opieki zdrowotnej (w tym szpitale i prywatne kliniki) i inne podmioty świadczące usługi opieki zdrowotnej

Poprawka

5. Służba zdrowia: punkty opieki zdrowotnej (w tym szpitale i prywatne kliniki) i inne podmioty świadczące usługi opieki zdrowotnej **z wyjątkiem prywatnych placówek opieki zdrowotnej oraz aptek, których obrót roczny nie przekracza 2 mln EUR.**

Or. en

Uzasadnienie

Roczny obrót wielu niezależnych placówek opieki zdrowotnej oraz aptek nie przekracza 2 mln EUR. W związku z tym incydenty mające wpływ na takie przedsiębiorstwa z dużym prawdopodobieństwem nie będą miały wystarczająco dużego zasięgu w zakresie skutków dla społeczeństwa w przeciwieństwie do sytuacji, gdy incydenty wpływają na większe przedsiębiorstwa. Objęcie takich przedsiębiorstw zakresem stosowania niniejszej dyrektywy byłoby nieproporcjonalne i miałoby negatywny wpływ na ich zdolność świadczenia wysokiej jakości usług w zakresie opieki zdrowotnej.