PARLAMENT EUROPEJSKI 2009 - 2014

Dokument z posiedzenia

A7-0103/2014

12.2.2014

***I
SPRAWOZDANIE

w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii
(COM(2013) 48 – C7-0035/2013 – 2013/0027(COD))

Komisja Rynku Wewnętrznego i Ochrony Konsumentów

Sprawozdawca: Andreas Schwab

Sprawozdawcy komisji opiniodawczej (*):
Pilar del Castillo Vera, Komisja Przemysłu, Badań Naukowych i Energii
Carl Schlyter, Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych

(*) Zaangażowane komisje – art. 50 Regulaminu

Objaśnienie używanych znaków

*	Procedura konsultacji
***	Procedura zgody
***I	Zwykła procedura ustawodawcza (pierwsze czytanie)
***II	Zwykła procedura ustawodawcza (drugie czytanie)
***III	Zwykła procedura ustawodawcza (trzecie czytanie)

(Wskazana procedura opiera się na podstawie prawnej zaproponowanej w projekcie aktu.)

Poprawki do projektu aktu

W poprawkach Parlamentu zmiany do projektu aktu zaznacza się ***wytłuszczonym drukiem i kursywą***. Oznakowanie *zwykłą kursywą* jest wskazówką dla służb technicznych dotyczącą propozycji korekty elementów projektu aktu w celu ustalenia tekstu końcowego (np. elementów w oczywisty sposób błędnych lub pominiętych w danej wersji językowej). Sugestie korekty wymagają zgody właściwych służb technicznych.

W poprawkach do aktów istniejących trzecia i czwarta linijka w nagłówku poprawki w projekcie aktu zawiera, odpowiednio, odniesienie do istniejącego aktu i postanowienia tego aktu, które ulega zmianie. Fragmenty przepisu aktu istniejącego, do którego Parlament wprowadza zmiany, a który nie został zmieniony w projekcie aktu, zaznacza się **wytłuszczonym drukiem**. Ewentualne skreślenia w obrębie takich fragmentów zaznaczane są w sposób następujący: **[...]**.

SPIS TREŚCI

Strona

(*) Zaangażowane komisje – art. 50 Regulaminu

PROJEKT REZOLUCJI USTAWODAWCZEJ PARLAMENTU EUROPEJSKIEGO

w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii
(COM(2013) 48 – C7-0035/2013 – 2013/0027(COD))

(Zwykła procedura ustawodawcza: pierwsze czytanie)

Parlament Europejski,

– uwzględniając wniosek Komisji przedstawiony Parlamentowi i Radzie (COM(2013)0048),

– uwzględniając art. 294 ust. 2 oraz art. 114 Traktatu o funkcjonowaniu Unii Europejskiej, zgodnie z którymi wniosek został przedstawiony Parlamentowi przez Komisję (C7–0035/2013),

– uwzględniając art. 294 ust. 3 Traktatu o funkcjonowaniu Unii Europejskiej,

– uwzględniając art.55 Regulaminu,

– uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego z dnia 22 maja 2013 r.[1],

– uwzględniając swoją rezolucję z dnia 12 września 2013 r. w sprawie strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń,[2],

– uwzględniając sprawozdanie Komisji Rynku Wewnętrznego i Ochrony Konsumentów oraz opinie Komisji Przemysłu, Badań Naukowych i Energii, Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych oraz Komisji Spraw Zagranicznych (A7-0103/2014),

1. przyjmuje poniższe stanowisko w pierwszym czytaniu;

2. zwraca się do Komisji o ponowne przekazanie mu sprawy, jeśli uzna ona za stosowne wprowadzić znaczące zmiany do swojego wniosku lub zastąpić go innym tekstem;

3. zobowiązuje swojego przewodniczącego do przekazania stanowiska Parlamentu Radzie i Komisji, a także parlamentom narodowym.

[1] Dz.U. C 0 z 0.0.0000, s. 0 /Dotychczas nieopublikowana w Dzienniku Urzędowym.
[2] Teksty przyjęte, P7_TA(2013)0376.

Poprawka 1

Wniosek dotyczący dyrektywy
Motyw 1

Tekst proponowany przez Komisję	*Poprawka*
(1) Sieci oraz systemy i usługi informatyczne pełnią w społeczeństwie istotną rolę. Ich niezawodność i bezpieczeństwo mają zasadnicze znaczenie dla działalności gospodarczej i dobrobytu społeczeństwa, a w szczególności dla funkcjonowania rynku wewnętrznego.	(1) Sieci oraz systemy i usługi informatyczne pełnią w społeczeństwie istotną rolę. Ich niezawodność i bezpieczeństwo mają zasadnicze znaczenie dla ***wolności i ogólnego bezpieczeństwa obywateli Unii, a także dla*** działalności gospodarczej i dobrobytu społeczeństwa, a w szczególności dla funkcjonowania rynku wewnętrznego.

Poprawka 2

Wniosek dotyczący dyrektywy
Motyw 2

Tekst proponowany przez Komisję	*Poprawka*
(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.	(2) Skala***, częstotliwość*** i ***konsekwencje*** incydentów w obszarze bezpieczeństwa stają się coraz większe i stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. ***Systemy te mogą się również stać łatwym celem umyślnych szkodliwych działań, mających na celu uszkodzenie lub przerwanie działania tych systemów.*** Incydenty takie mogą utrudniać prowadzenie działalności gospodarczej, powodować znaczne straty finansowe, podważać zaufanie użytkowników ***i inwestorów*** oraz powodować znaczne straty w gospodarce Unii***, a w konsekwencji stanowić zagrożenie dla dobrobytu obywateli Unii oraz zdolności państw członkowskich do zapewnienia własnej ochrony oraz bezpieczeństwa infrastruktury krytycznej***.

Poprawka 3

Wniosek dotyczący dyrektywy
Motyw 3

Tekst proponowany przez Komisję	*Poprawka*
	(3a) Zważywszy, że do awarii systemów najczęściej dochodzi nadal z przyczyn niezamierzonych, jak przyczyny naturalne lub błędy ludzkie, infrastruktura powinna być odporna zarówno na zamierzone, jak i niezamierzone zakłócenia, a operatorzy infrastruktury krytycznej powinni projektować systemy oparte na zasadzie odporności.

Poprawka 4

Wniosek dotyczący dyrektywy
Motyw 4

Tekst proponowany przez Komisję	*Poprawka*
(4) Na poziomie Unii należy ustanowić mechanizm współpracy, który umożliwi wymianę informacji i podejmowanie skoordynowanych działań w zakresie wykrywania i reagowania w odniesieniu do bezpieczeństwa sieci i informacji. Aby mechanizm ten był skuteczny i dostępny dla wszystkich, konieczne jest, by wszystkie państwa członkowskie posiadały minimalne zdolności i strategię zapewniające wysoki poziom bezpieczeństwa sieci i informacji na ich terytorium. Aby promować kulturę wspierającą przeciwdziałanie zagrożeniom i zapewnić zgłaszanie najpoważniejszych incydentów, należy wprowadzić minimalne wymogi w zakresie bezpieczeństwa również w odniesieniu do ***organów administracji publicznej i*** operatorów ***krytycznej*** infrastruktury teleinformatycznej.	(4) Na poziomie Unii należy ustanowić mechanizm współpracy, który umożliwi wymianę informacji i podejmowanie skoordynowanych działań w zakresie ***zapobiegania,*** wykrywania i reagowania w odniesieniu do bezpieczeństwa sieci i informacji. Aby mechanizm ten był skuteczny i dostępny dla wszystkich, konieczne jest, by wszystkie państwa członkowskie posiadały minimalne zdolności i strategię zapewniające wysoki poziom bezpieczeństwa sieci i informacji na ich terytorium. Aby promować kulturę wspierającą przeciwdziałanie zagrożeniom i zapewnić zgłaszanie najpoważniejszych incydentów, należy wprowadzić minimalne wymogi w zakresie bezpieczeństwa również w odniesieniu do ***przynajmniej niektórych rynkowych*** operatorów infrastruktury teleinformatycznej. ***Należy zachęcać spółki notowane na giełdzie do dobrowolnego ujawniania incydentów w swoich sprawozdaniach finansowych.***

Ramy prawne powinny opierać się na potrzebie zabezpieczenia prywatności i integralności obywateli. Sieci ostrzegania o zagrożeniach dla infrastruktury krytycznej należy rozszerzyć na podmioty gospodarcze objęte niniejszą dyrektywą.

Poprawka 5

Wniosek dotyczący dyrektywy
Motyw 4 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(4a) Podczas gdy organy administracji publicznej – z uwagi na swoją misję publiczną – powinny zarządzać własnymi sieciami i systemami informatycznymi oraz chronić je z należytą starannością, niniejsza dyrektywa powinna skupić się na infrastrukturze krytycznej, która ma zasadnicze znaczenie dla utrzymania kluczowych działań gospodarczych i społecznych w dziedzinach energetyki, transportu, bankowości, infrastruktury rynków finansowych czy opieki zdrowotnej. Z zakresu niniejszej dyrektywy należy wyłączyć twórców oprogramowania i producentów sprzętu.

Poprawka 6

Wniosek dotyczący dyrektywy
Motyw 4 b (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(4b) Współpracę i koordynację między właściwymi organami unijnymi z wysokim przedstawicielem/wiceprzewodniczącym Komisji – odpowiedzialnymi za wspólną politykę zagraniczną i bezpieczeństwa oraz wspólną politykę bezpieczeństwa i obrony – oraz koordynatorem UE ds.

	zwalczania terroryzmu należy zagwarantować w przypadkach, w których charakter incydentów mających znaczące konsekwencje uważa się za zewnętrzny lub terrorystyczny.

Poprawka 7

Wniosek dotyczący dyrektywy
Motyw 6

Tekst proponowany przez Komisję	*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.	(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 podmiotów gospodarczych uniemożliwia z kolei ustanowienie globalnego i skutecznego mechanizmu współpracy na poziomie Unii. ***Uniwersytety i placówki badawcze odgrywają zasadniczą rolę w pobudzaniu badań, rozwoju i innowacyjności w tych obszarach i należy udzielać im odpowiedniego wsparcia finansowego.***

Poprawka 8

Wniosek dotyczący dyrektywy
Motyw 7

Tekst proponowany przez Komisję	*Poprawka*
(7) Skuteczne reagowanie na wyzwania związane z zapewnieniem bezpieczeństwa	(7) Skuteczne reagowanie na wyzwania związane z zapewnieniem bezpieczeństwa

sieci i systemów informatycznych wymaga zatem przyjęcia całościowego podejścia na poziomie Unii, które będzie obejmować wprowadzenie wymogów dotyczących budowania i planowania wspólnych minimalnych zdolności, wymianę informacji i koordynację działań oraz wprowadzenie wspólnych minimalnych wymogów w zakresie bezpieczeństwa ***dla wszystkich podmiotów gospodarczych, których dotyczy ten problem, oraz dla organów administracji publicznej***.	sieci i systemów informatycznych wymaga zatem przyjęcia całościowego podejścia na poziomie Unii, które będzie obejmować wprowadzenie wymogów dotyczących budowania i planowania wspólnych minimalnych zdolności, ***rozwijanie dostatecznych umiejętności z zakresu bezpieczeństwa cybernetycznego,*** wymianę informacji i koordynację działań oraz wprowadzenie wspólnych minimalnych wymogów w zakresie bezpieczeństwa. ***Minimalne wspólne normy należy stosować zgodnie z odpowiednimi zaleceniami grup koordynacji bezpieczeństwa cybernetycznego.***

Poprawka 9

Wniosek dotyczący dyrektywy
Motyw 8

Tekst proponowany przez Komisję	*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.	(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.

Uzasadnienie

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

Poprawka 10

Wniosek dotyczący dyrektywy
Motyw 9

Tekst proponowany przez Komisję	*Poprawka*
(9) W celu osiągnięcia i utrzymania wspólnego wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych każde państwo członkowskie powinno posiadać krajową strategię w zakresie bezpieczeństwa sieci i informacji określającą cele strategiczne i konkretne działania, które należy wdrożyć. Na poziome krajowym należy opracować spełniające zasadnicze wymagania plany współpracy w zakresie bezpieczeństwa sieci i informacji, tak aby osiągnąć poziom zdolności reagowania umożliwiający skuteczną i sprawną współpracę na poziomach krajowym i unijnym w przypadku wystąpienia incydentów.	(9) W celu osiągnięcia i utrzymania wspólnego wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych każde państwo członkowskie powinno posiadać krajową strategię w zakresie bezpieczeństwa sieci i informacji określającą cele strategiczne i konkretne działania, które należy wdrożyć. W oparciu o minimalne wymogi ustanowione w niniejszej dyrektywie na poziomie krajowym należy opracować spełniające zasadnicze wymagania plany współpracy w zakresie bezpieczeństwa sieci i informacji, tak aby osiągnąć poziom zdolności reagowania umożliwiający skuteczną i sprawną współpracę na poziomach krajowym i unijnym w przypadku wystąpienia incydentów, przy poszanowaniu i ochronie życia prywatnego i danych osobowych. ***Każde państwo członkowskie powinno zatem być zobowiązane do wypełniania wspólnych norm dotyczących formatu i wymienialności danych, które mają być udostępniane i oceniane. Państwa członkowskie powinny mieć możliwość zwrócenia się do Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) o pomoc w opracowywaniu***

krajowych strategii w zakresie bezpieczeństwa sieci i informacji na podstawie wspólnej minimalnej strategii w zakresie bezpieczeństwa sieci i informacji.

Poprawka 11

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 wyznaczanie 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. Właściwe organy i krajowe pojedyncze punkty kontaktowe powinny być podmiotami cywilnymi podlegającymi pełnej kontroli demokratycznej i nie powinny wypełniać żadnych zadań w dziedzinie wywiadu, egzekwowania prawa czy obrony ani też być organizacyjnie

powiązane w żadnej formie z podmiotami działającymi aktywnie w tych obszarach.

Poprawka 12

Wniosek dotyczący dyrektywy
Motyw 11

Tekst proponowany przez Komisję	*Poprawka*
(11) Wszystkie państwa członkowskie powinny zostać odpowiednio wyposażone, zarówno pod względem zdolności technicznych, jak i możliwości organizacyjnych, w celu zapobiegania incydentom i zagrożeniom dotyczącym sieci i systemów informatycznych, wykrywania ich, reagowania na nie i łagodzenia ich skutków. We wszystkich państwach członkowskich należy zatem ustanowić sprawnie funkcjonujące i spełniające zasadnicze wymagania zespoły reagowania na incydenty komputerowe, które zagwarantują skuteczne i kompatybilne zdolności reagowania na incydenty i zagrożenia oraz zapewnią skuteczną współpracę na poziomie unijnym.	(11) Wszystkie państwa członkowskie ***i podmioty gospodarcze*** powinny zostać odpowiednio wyposażone, zarówno pod względem zdolności technicznych, jak i możliwości organizacyjnych, w celu zapobiegania incydentom i zagrożeniom dotyczącym sieci i systemów informatycznych, wykrywania ich, reagowania na nie i łagodzenia ich skutków ***w dowolnym momencie***. ***Systemy bezpieczeństwa administracji publicznej powinny być bezpieczne i podlegać demokratycznej kontroli i nadzorowi. Wspólnie wymagane wyposażenie i zdolności powinny odpowiadać wspólnie uzgodnionym normom technicznym oraz standardowym procedurom działania.*** We wszystkich państwach członkowskich należy zatem ustanowić sprawnie funkcjonujące i spełniające zasadnicze wymagania zespoły reagowania na incydenty komputerowe ***(CERT)***, które zagwarantują skuteczne i kompatybilne zdolności reagowania na incydenty i zagrożenia oraz zapewnią skuteczną współpracę na poziomie unijnym. ***CERT powinny mieć możliwość interakcji na podstawie wspólnych standardów technicznych i standardowych procedur działania. Z uwagi na różne cechy istniejących CERT, które odpowiadają różnym potrzebom tematycznym i podmiotom, państwa członkowskie powinny zagwarantować, że każdy sektor wymieniony w wykazie podmiotów gospodarczych określonych w niniejszej***

dyrektywie jest obsługiwany przez co najmniej jeden CERT. W odniesieniu do współpracy transgranicznej CERT państwa członkowskie powinny dopilnować, aby CERT posiadały środki wystarczające do udziału w już działających międzynarodowych i unijnych sieciach współpracy.

Uzasadnienie

Należy zapewnić interoperacyjność.

Poprawka 13

Wniosek dotyczący dyrektywy
Motyw 12

Tekst proponowany przez Komisję	*Poprawka*
(12) Opierając się na znacznych postępach dokonanych w ramach europejskiego forum państw członkowskich (EFMS), które umożliwiły prowadzenie dialogu i wymianę doświadczeń dotyczących sprawdzonych rozwiązań, w tym opracowywanie zasad współpracy na wypadek kryzysów cybernetycznych w Europie, państwa członkowskie i Komisja powinny stworzyć sieć w celu zapewnienia ich stałej komunikacji i wsparcia ich współpracy. Ten bezpieczny i skuteczny mechanizm współpracy powinien umożliwić uporządkowaną i skoordynowaną wymianę informacji, wykrywanie incydentów oraz reagowanie na nie na poziomie Unii.	(12) Opierając się na znacznych postępach dokonanych w ramach europejskiego forum państw członkowskich (EFMS), które umożliwiły prowadzenie dialogu i wymianę doświadczeń dotyczących sprawdzonych rozwiązań, w tym opracowywanie zasad współpracy na wypadek kryzysów cybernetycznych w Europie, państwa członkowskie i Komisja powinny stworzyć sieć w celu zapewnienia ich stałej komunikacji i wsparcia ich współpracy. Ten bezpieczny i skuteczny mechanizm współpracy***, w którym zapewnia się w stosownych przypadkach udział podmiotów gospodarczych,*** powinien umożliwić uporządkowaną i skoordynowaną wymianę informacji, wykrywanie incydentów oraz reagowanie na nie na poziomie Unii.

Poprawka 14

Wniosek dotyczący dyrektywy
Motyw 13

Tekst proponowany przez Komisję	*Poprawka*
(13) ***Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (***ENISA***)*** powinna wspierać działania państw członkowskich i Komisji poprzez zapewnianie wiedzy specjalistycznej i doradztwa oraz poprzez ułatwianie wymiany najlepszych praktyk. W szczególności Komisja ***powinna*** konsultować się z ENISA przy stosowaniu niniejszej dyrektywy. W celu zapewnienia skutecznego i terminowego informowania państw członkowskich i Komisji wczesne ostrzeżenia dotyczące incydentów i zagrożeń należy zgłaszać poprzez sieć współpracy. Aby budować zdolności i wiedzę wśród państw członkowskich, sieć współpracy powinna również służyć jako narzędzie wymiany najlepszych praktyk, pomagać członkom w budowaniu zdolności oraz kierować organizacją wzajemnej weryfikacji i ćwiczeń w zakresie bezpieczeństwa sieci i informacji.	(13) ENISA powinna wspierać działania państw członkowskich i Komisji poprzez zapewnianie wiedzy specjalistycznej i doradztwa oraz poprzez ułatwianie wymiany najlepszych praktyk. W szczególności Komisja ***i państwa członkowskie powinny*** konsultować się z ENISA przy stosowaniu niniejszej dyrektywy. W celu zapewnienia skutecznego i terminowego informowania państw członkowskich i Komisji wczesne ostrzeżenia dotyczące incydentów i zagrożeń należy zgłaszać poprzez sieć współpracy. Aby budować zdolności i wiedzę wśród państw członkowskich, sieć współpracy powinna również służyć jako narzędzie wymiany najlepszych praktyk, pomagać członkom w budowaniu zdolności oraz kierować organizacją wzajemnej weryfikacji i ćwiczeń w zakresie bezpieczeństwa sieci i informacji.

Poprawka 15

Wniosek dotyczący dyrektywy
Motyw 13 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(13a) W stosownych przypadkach podczas stosowania przepisów niniejszej dyrektywy państwa członkowskie powinny móc wykorzystywać lub dostosowywać istniejące struktury lub strategie organizacyjne.

Poprawka 16

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 techniczne i finansowe oraz zasoby ludzkie, jak również ich infrastruktura łączności, gwarantują ich skuteczne, sprawne i bezpieczne uczestnictwo w sieci.	(14) Aby umożliwić wymianę szczególnie chronionych i poufnych informacji w ramach sieci współpracy, należy zapewnić bezpieczną infrastrukturę do wymiany informacji. ***W tym celu należy w pełni wykorzystywać istniejące w Unii struktury.*** 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 ***przy zastosowaniu przejrzystych metod***.

Poprawka 17

Wniosek dotyczący dyrektywy
Motyw 15

Tekst proponowany przez Komisję	*Poprawka*
(15) Ponieważ większość sieci i systemów informatycznych eksploatowana jest przez podmioty prywatne, niezbędna jest współpraca między sektorem publicznym i prywatnym. Podmioty gospodarcze należy zachęcać do tworzenia własnych nieformalnych mechanizmów współpracy w celu zapewnienia bezpieczeństwa sieci i informacji. Powinny one również współpracować z sektorem publicznym oraz dzielić się ***z nim*** informacjami i najlepszymi praktykami ***w zamian za*** wsparcie operacyjne w przypadku incydentów.	(15) Ponieważ większość sieci i systemów informatycznych eksploatowana jest przez podmioty prywatne, niezbędna jest współpraca między sektorem publicznym i prywatnym. Podmioty gospodarcze należy zachęcać do tworzenia własnych nieformalnych mechanizmów współpracy w celu zapewnienia bezpieczeństwa sieci i informacji. Powinny one również współpracować z sektorem publicznym oraz dzielić się ***obustronnie*** informacjami i najlepszymi praktykami***, co obejmuje także wzajemną wymianę odpowiednich informacji,*** wsparcie operacyjne ***i informacje analizowane pod kątem strategicznym*** w przypadku incydentów. ***W***

	celu aktywnego zachęcania do dzielenia się informacjami oraz najlepszymi praktykami konieczne jest zapewnienie, by podmioty gospodarcze uczestniczące w wymianie nie doświadczały strat w wyniku tej współpracy. Konieczne są odpowiednie zabezpieczenia w celu zapewnienia, by tego rodzaju współpraca nie narażała takich podmiotów na wyższe ryzyko braku zgodności lub na nowe zobowiązania na podstawie m.in. prawa konkurencji, własności intelektualnej, ochrony danych czy cyberprzestępczości oraz by nie narażała ich na podwyższone ryzyko operacyjne lub związane z bezpieczeństwem.

Poprawka 18

Wniosek dotyczący dyrektywy
Motyw 16

Tekst proponowany przez Komisję	*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***.	(16) W celu zapewnienia przejrzystości i w celu odpowiedniego informowania obywateli ***Unii*** i ***unijnych*** podmiotów gospodarczych ***pojedyncze punkty kontaktowe*** powinny założyć wspólną ***ogólnounijną*** stronę internetową, na której publikowane będą niemające poufnego charakteru informacje na temat incydentów***, zagrożeń*** i ***sposobów ich łagodzenia oraz gdzie będzie się udzielać porad dotyczących odpowiedniej obsługi technicznej***. ***Informacje na stronie internetowej powinny być dostępne bez względu na rodzaj urządzenia. Wszelkie dane osobowe publikowane na tej stronie internetowej powinny ograniczać się do tego, co niezbędne, i być jak najbardziej anonimowe.***

Poprawka 19

Wniosek dotyczący dyrektywy
Motyw 18

Tekst proponowany przez Komisję	*Poprawka*
(18) Na podstawie zwłaszcza krajowych doświadczeń w zarządzaniu kryzysowym i we współpracy z ENISA Komisja i państwa członkowskie powinny opracować unijny plan współpracy w zakresie bezpieczeństwa sieci i informacji określający mechanizmy współpracy służące ***do zwalczania zagrożeń i incydentów***. Plan ten należy odpowiednio uwzględniać podczas korzystania z systemu wczesnego ostrzegania w ramach sieci współpracy.	(18) Na podstawie zwłaszcza krajowych doświadczeń w zarządzaniu kryzysowym i we współpracy z ENISA Komisja i państwa członkowskie powinny opracować unijny plan współpracy w zakresie bezpieczeństwa sieci i informacji określający mechanizmy współpracy ***oraz najlepsze praktyki i wzorce działania*** służące ***zapobieganiu zagrożeniom i incydentom oraz ich wykrywaniu, zgłaszaniu i zwalczaniu***. Plan ten należy odpowiednio uwzględniać podczas korzystania z systemu wczesnego ostrzegania w ramach sieci współpracy.

Poprawka 20

Wniosek dotyczący dyrektywy
Motyw 19

Tekst proponowany przez Komisję	*Poprawka*
(19) Przekazywanie wczesnych ostrzeżeń w ramach sieci powinno być wymagane tylko w przypadku, gdy skala i waga danego incydentu lub zagrożenia są lub mogą być w przyszłości na tyle znaczące, że konieczna jest wymiana informacji lub koordynacja reakcji na poziomie Unii. Wczesne ostrzeżenia powinny być zatem ograniczone do ***rzeczywistych lub potencjalnych*** incydentów lub zagrożeń, które się szybko rozwijają, przekraczają krajowe zdolności reagowania lub mają wpływ na więcej niż jedno państwo członkowskie. W celu umożliwienia właściwej oceny wszystkie informacje niezbędne do oceny zagrożenia lub incydentu należy przekazywać do sieci współpracy.	(19) Przekazywanie wczesnych ostrzeżeń w ramach sieci powinno być wymagane tylko w przypadku, gdy skala i waga danego incydentu lub zagrożenia są lub mogą być w przyszłości na tyle znaczące, że konieczna jest wymiana informacji lub koordynacja reakcji na poziomie Unii. Wczesne ostrzeżenia powinny być zatem ograniczone do incydentów lub zagrożeń, które się szybko rozwijają, przekraczają krajowe zdolności reagowania lub mają wpływ na więcej niż jedno państwo członkowskie. W celu umożliwienia właściwej oceny wszystkie informacje niezbędne do oceny zagrożenia lub incydentu należy przekazywać do sieci współpracy.

Poprawka 21

Wniosek dotyczący dyrektywy
Motyw 20

Tekst proponowany przez Komisję	*Poprawka*
(20) Po otrzymaniu wczesnego ostrzeżenia i dokonaniu jego oceny ***właściwe organy*** powinny uzgodnić skoordynowaną reakcję zgodnie z unijnym planem współpracy w zakresie bezpieczeństwa sieci i informacji. O środkach przyjętych na poziomie krajowym w wyniku skoordynowanej reakcji należy poinformować ***właściwe organy*** oraz Komisję.	(20) Po otrzymaniu wczesnego ostrzeżenia i dokonaniu jego oceny ***pojedyncze punkty kontaktowe*** powinny uzgodnić skoordynowaną reakcję zgodnie z unijnym planem współpracy w zakresie bezpieczeństwa sieci i informacji. O środkach przyjętych na poziomie krajowym w wyniku skoordynowanej reakcji należy poinformować ***pojedyncze punkty kontaktowe, ENISA*** oraz Komisję.

Poprawka 22

Wniosek dotyczący dyrektywy
Motyw 21

Tekst proponowany przez Komisję	*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.	(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 23

Wniosek dotyczący dyrektywy
Motyw 22

Tekst proponowany przez Komisję	*Poprawka*
(22) Odpowiedzialność za zapewnienie bezpieczeństwa sieci i informacji w dużym stopniu spoczywa na ***organach administracji publicznej i*** podmiotach gospodarczych. Za pomocą stosownych wymogów regulacyjnych i dobrowolnych praktyk branżowych należy wspierać i rozwijać kulturę przeciwdziałania zagrożeniom, obejmującą przeprowadzanie ocen zagrożenia i wdrażanie środków bezpieczeństwa stosownych do ***danego*** zagrożenia. Stworzenie równych warunków działania ma również kluczowe znaczenie dla skutecznego funkcjonowania sieci współpracy w celu zapewnienia skutecznej współpracy ze strony wszystkich państw członkowskich.	(22) Odpowiedzialność za zapewnienie bezpieczeństwa sieci i informacji w dużym stopniu spoczywa na podmiotach gospodarczych. Za pomocą stosownych wymogów regulacyjnych i dobrowolnych praktyk branżowych należy wspierać i rozwijać kulturę przeciwdziałania zagrożeniom, ***ścisłej współpracy i zaufania,*** obejmującą przeprowadzanie ocen zagrożenia i wdrażanie środków bezpieczeństwa stosownych do zagrożenia ***i incydentów, zarówno umyślnych, jak i przypadkowych***. Stworzenie ***godnych zaufania,*** równych warunków działania ma również kluczowe znaczenie dla skutecznego funkcjonowania sieci współpracy w celu zapewnienia skutecznej współpracy ze strony wszystkich państw członkowskich.

Poprawka 24

Wniosek dotyczący dyrektywy
Motyw 24

Tekst proponowany przez Komisję	*Poprawka*
(24) Obowiązki te powinny obejmować nie tylko sektor łączności elektronicznej, lecz również głównych dostawców usług społeczeństwa informacyjnego, określonych w dyrektywie 98/34/WE Parlamentu Europejskiego i Rady z dnia 22 czerwca 1998 r. ustanawiającej procedurę udzielania informacji w dziedzinie norm i przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego[27], na których opierają się pochodne usługi społeczeństwa informacyjnego oraz działania w prowadzone w internecie, takie jak platformy handlu elektronicznego, internetowe portale płatnicze, portale społecznościowe, wyszukiwarki, usługi	(24) Obowiązki te powinny obejmować nie tylko sektor łączności elektronicznej, lecz również ***operatorów infrastruktury, którzy są w dużym stopniu uzależnieni od technologii informacyjnych i komunikacyjnych i którzy mają kluczowe znaczenie dla utrzymania istotnych funkcji gospodarczych lub społecznych, takich jak dostawy energii elektrycznej i gazu, usługi transportowe, działalność instytucji kredytowych, infrastruktura rynków finansowych i opieka zdrowotna. Zakłócenia tych sieci i systemów informatycznych miałyby wpływ na rynek wewnętrzny. O ile obowiązki ustanowione w niniejszej dyrektywie nie powinny obejmować*** głównych dostawców usług

chmur obliczeniowych***,*** sklepy z aplikacjami. ***Zakłócenia tych podstawowych usług społeczeństwa informacyjnego uniemożliwiają świadczenie innych usług społeczeństwa informacyjnego***, dla ***których stanowią one podstawę. Twórcy oprogramowania i producenci sprzętu nie są dostawcami usług społeczeństwa informacyjnego, a zatem nie są oni objęci zakresem powyższych przepisów. Obowiązki te powinny również zostać rozszerzone na organy administracji publicznej oraz operatorów infrastruktury krytycznej, którzy są w dużym stopniu uzależnieni od technologii informacyjnych i komunikacyjnych i którzy mają kluczowe znaczenie dla utrzymania istotnych funkcji gospodarczych i społecznych, takich jak dostawy energii elektrycznej i gazu, usługi transportowe oraz działalność instytucji kredytowych, giełd papierów wartościowych i placówek opieki zdrowotnej. Zakłócenia tych sieci i systemów informatycznych miałyby wpływ na rynek wewnętrzny.***

społeczeństwa informacyjnego, określonych w dyrektywie 98/34/WE Parlamentu Europejskiego i Rady z dnia 22 czerwca 1998 r. ustanawiającej procedurę udzielania informacji w dziedzinie norm i przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego[27], na których opierają się pochodne usługi społeczeństwa informacyjnego oraz działania w prowadzone w internecie, takie jak platformy handlu elektronicznego, internetowe portale płatnicze, portale społecznościowe, wyszukiwarki, usługi chmur obliczeniowych ***ogólnie lub*** sklepy z aplikacjami***, mogą one na zasadzie dobrowolności informować właściwy organ lub pojedynczy punkt kontaktowy o tych incydentach związanych z bezpieczeństwem sieci, które uznają za stosowne***. ***Na ile to możliwe, właściwy organ lub pojedynczy punkt kontaktowy powinien przedstawić podmiotom gospodarczym, które powiadomiły o incydencie, informacje przeanalizowane pod kątem strategicznym, które pomogą przezwyciężyć zagrożenie*** dla ***bezpieczeństwa.***

Poprawka 25

Wniosek dotyczący dyrektywy
Motyw 24 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(24a) Podczas gdy dostawcy sprzętu i oprogramowania nie są podmiotami gospodarczymi porównywalnymi z tymi, którzy są objęci niniejszą dyrektywą, ich produkty sprzyjają zapewnieniu bezpieczeństwa sieci i systemów informatycznych. Odgrywają zatem ważną rolę w umożliwieniu podmiotom gospodarczym zabezpieczenia ich infrastruktury sieci i infrastruktury informatycznej. Jako że sprzęt i

	oprogramowanie podlega już obowiązującym zasadom odpowiedzialności za produkt, państwa członkowskie powinny dopilnować egzekwowania tych zasad.

Poprawka 26

Wniosek dotyczący dyrektywy
Motyw 25

Tekst proponowany przez Komisję	*Poprawka*
(25) Nałożenie na ***organy administracji publicznej i*** podmioty gospodarcze obowiązku wprowadzenia środków organizacyjnych i technicznych nie powinno wiązać się z koniecznością zaprojektowania, opracowania i wyprodukowania specjalnego komercyjnego produktu informatycznego w określony sposób.	(25) Nałożenie na podmioty gospodarcze obowiązku wprowadzenia środków organizacyjnych i technicznych nie powinno wiązać się z koniecznością zaprojektowania, opracowania i wyprodukowania specjalnego komercyjnego produktu informatycznego w określony sposób.

Poprawka 27

Wniosek dotyczący dyrektywy
Motyw 26

Tekst proponowany przez Komisję	*Poprawka*
(26) ***Organy administracji publicznej oraz*** podmioty gospodarcze powinny zapewnić bezpieczeństwo sieci i systemów, które są pod ich kontrolą. Dotyczy to przede wszystkim sieci i systemów prywatnych, które są zarządzane przez wewnętrzny personel informatyczny lub w przypadku których zapewnienie bezpieczeństwa zlecono na zewnątrz. Wymogi w zakresie bezpieczeństwa i zgłaszania incydentów powinny mieć zastosowanie do odpowiednich podmiotów gospodarczych ***i organów administracji publicznej*** bez względu na to, czy one same zapewniają obsługę swoich sieci i systemów informatycznych, czy też zlecają tę obsługę	(26) Podmioty gospodarcze powinny zapewnić bezpieczeństwo sieci i systemów, które są pod ich kontrolą. Dotyczy to przede wszystkim sieci i systemów prywatnych, które są zarządzane przez wewnętrzny personel informatyczny lub w których przypadku zapewnienie bezpieczeństwa zlecono na zewnątrz. Wymogi w zakresie bezpieczeństwa i zgłaszania incydentów powinny mieć zastosowanie do odpowiednich podmiotów gospodarczych bez względu na to, czy one same zapewniają obsługę swoich sieci i systemów informatycznych, czy też zlecają tę obsługę innym podmiotom.

innym podmiotom.

Poprawka 28

Wniosek dotyczący dyrektywy
Motyw 28

Tekst proponowany przez Komisję	*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.	(28) Właściwe organy ***i pojedyncze punkty kontaktowe*** powinny zwracać należytą uwagę na zachowanie nieformalnych i bezpiecznych kanałów wymiany informacji między podmiotami gospodarczymi i między sektorami publicznym i prywatnym. ***Właściwe organy oraz pojedyncze punkty kontaktowe powinny informować producentów i usługodawców danych produktów i usług ICT o zgłoszonych im incydentach mających znaczące konsekwencje.*** Decyzje o informowaniu społeczeństwa o incydentach zgłoszonych właściwym organom ***i pojedynczym punktom kontaktowym*** 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 podmioty gospodarcze zgłaszające incydenty. Wykonując obowiązki w zakresie powiadamiania, właściwe organy ***i pojedyncze punkty kontaktowe*** powinny zwracać szczególną uwagę na potrzebę zachowania poufności w odniesieniu do informacji dotyczących słabych punktów produktów, aż do momentu ***wdrożenia*** stosownych rozwiązań problemów bezpieczeństwa. ***Z zasady pojedyncze punkty kontaktowe nie powinny ujawniać danych osobowych osób zaangażowanych w incydenty. Pojedyncze punkty kontaktowe powinny ujawniać dane osobowe wyłącznie wtedy, kiedy ujawnienie takich danych jest niezbędne i współmierne do celu, w***

którym są ujawniane.

Poprawka 29

Wniosek dotyczący dyrektywy
Motyw 29

Tekst proponowany przez Komisję	*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.	(29) Właściwe organy powinny dysponować niezbędnymi środkami do wykonywania swoich obowiązków, w tym uprawnieniami do uzyskiwania wystarczających informacji od podmiotów gospodarczych, w celu oceny poziomu bezpieczeństwa sieci i systemów informatycznych, ***zmierzenia liczby, skali i zakresu incydentów,*** jak również wiarygodnymi i pełnymi danymi na temat incydentów, które mają wpływ na funkcjonowanie sieci i systemów informatycznych.

Poprawka 30

Wniosek dotyczący dyrektywy
Motyw 30

Tekst proponowany przez Komisję	*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 i organami ścigania ***powinna*** stanowić część skutecznej i kompleksowej reakcji na zagrożenie związane z możliwością wystąpienia incydentu zagrażającego bezpieczeństwu. Wspieranie rozwoju bezpiecznego, chronionego i bardziej odpornego środowiska wymaga w szczególności systematycznego zgłaszania organom	(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*** i organami ścigania ***oraz współpraca z EC3 (ośrodek Europolu ds. cyberprzestępczości) i z ENISA powinny*** stanowić część skutecznej i kompleksowej reakcji na zagrożenie związane z możliwością wystąpienia incydentu zagrażającego bezpieczeństwu. Wspieranie rozwoju bezpiecznego,

ścigania poważnych incydentów, które mogą mieć charakter przestępczy. Poważne incydenty o charakterze przestępczym należy oceniać w świetle prawa UE w zakresie cyberprzestępczości.

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.

Poprawka 31

Wniosek dotyczący dyrektywy
Motyw 31

Tekst proponowany przez Komisję	*Poprawka*
(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 incydentów***, które stanowią*** naruszenie danych osobowych, zmniejszając tym	(31) W wyniku incydentów w wielu przypadkach istnieje niebezpieczeństwo naruszenia danych osobowych. ***Państwa członkowskie i podmioty gospodarcze powinny chronić przechowywane, przetwarzane i przekazywane dane osobowe przed przypadkowym lub bezprawnym zniszczeniem, przypadkową utratą lub zmianą, a także nieupoważnionym czy bezprawnym przechowywaniem, dostępem, ujawnianiem lub rozpowszechnianiem. Powinny też zapewnić wdrożenie polityki bezpieczeństwa w odniesieniu do przetwarzania danych osobowych. W*** tym kontekście właściwe organy***, pojedyncze punkty kontaktowe*** oraz organy ochrony danych 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***. Obowiązek zgłaszania incydentów zagrażających bezpieczeństwu ***należy wypełniać*** w sposób, który minimalizuje obciążenia administracyjne w przypadku, gdy incydent zagrażający bezpieczeństwu stanowi również

samym obciążenia administracyjne dla przedsiębiorstw i organów administracji publicznej.

naruszenie ***zasad dotyczących*** danych osobowych***, które wymaga zgłoszenia zgodnie z prawem Unii*** w zakresie ***ochrony*** danych. ***ENISA powinna udzielić pomocy, opracowując*** mechanizmy wymiany informacji ***i jednolity wzór formularza***, ***które ułatwiłyby*** zgłaszanie incydentów ***stanowiących*** naruszenie danych osobowych, zmniejszając tym samym obciążenia administracyjne dla przedsiębiorstw i organów administracji publicznej.

Poprawka 32

Wniosek dotyczący dyrektywy
Motyw 32

Tekst proponowany przez Komisję	*Poprawka*
(32) Normalizacja wymogów w zakresie bezpieczeństwa jest procesem napędzanym przez rynek. W celu zapewnienia spójnego stosowania norm bezpieczeństwa państwa członkowskie powinny wspierać dążenie do zgodności lub zbieżności z określonymi normami w celu zapewnienia wysokiego poziomu bezpieczeństwa na poziomie Unii. W tym celu ***konieczne*** może być przygotowanie ujednoliconych norm, czego należy dokonać zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniającym dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylającym decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE[29].	(32) Normalizacja wymogów w zakresie bezpieczeństwa jest ***dobrowolnym*** procesem napędzanym przez rynek***, który powinien umożliwić podmiotom gospodarczym korzystanie z alternatywnych środków w celu osiągnięcia co najmniej podobnych wyników***. W celu zapewnienia spójnego stosowania norm bezpieczeństwa państwa członkowskie powinny wspierać dążenie do zgodności lub zbieżności z określonymi ***interoperacyjnymi*** normami w celu zapewnienia wysokiego poziomu bezpieczeństwa na poziomie Unii. W tym celu ***należy rozważyć stosowanie otwartych norm międzynarodowych do bezpieczeństwa sieci i informacji lub opracowanie takich narzędzi. Kolejnym koniecznym krokiem naprzód*** może być przygotowanie ujednoliconych norm, czego należy dokonać zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniającym dyrektywy Rady 89/686/EWG i

	93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylającym decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE[29]. ***W szczególności należy upoważnić ETSI, CEN i CENELEC do proponowania skutecznych i wydajnych otwartych unijnych norm bezpieczeństwa, w których unika się preferencji technologicznych w jak najwyższym stopniu i którymi mogą łatwo zarządzać małe i średnie podmioty gospodarcze. Normy międzynarodowe dotyczące bezpieczeństwa cybernetycznego należy dokładnie sprawdzić w celu zapewnienia, że nie zostały one naruszone, ustanawiają odpowiednie poziomy bezpieczeństwa, tym samym gwarantując, że zalecona zgodność z normami bezpieczeństwa cybernetycznego zwiększa, a nie zmniejsza ogólny poziom tego bezpieczeństwa w Unii.***
[29] Dz.U. L 316 z 14.11.2012, s. 12.	[29] Dz.U. L 316 z 14.11.2012, s. 12.

Poprawka 33

Wniosek dotyczący dyrektywy
Motyw 33

Tekst proponowany przez Komisję	*Poprawka*
(33) Komisja powinna okresowo dokonywać przeglądu niniejszej dyrektywy, w szczególności w celu sprawdzenia, czy konieczne jest wprowadzenie zmian w świetle zmieniających się technologii i warunków rynkowych.	(33) Komisja powinna okresowo dokonywać przeglądu niniejszej dyrektywy, ***w drodze konsultacji ze wszystkimi zainteresowanymi stronami,*** w szczególności w celu sprawdzenia, czy konieczne jest wprowadzenie zmian w świetle zmieniających się technologii i warunków ***społecznych, politycznych lub*** rynkowych.

Poprawka 34

Wniosek dotyczący dyrektywy
Motyw 34

Tekst proponowany przez Komisję	*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 ***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***.	(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 ***wspólnego zestawu norm w zakresie wzajemnych połączeń i bezpieczeństwa dla potrzeb bezpiecznej infrastruktury służącej do*** wymiany informacji ***oraz*** sprecyzowania, które zdarzenia wymagają wczesnego ostrzegania.

Poprawka 35

Wniosek dotyczący dyrektywy
Motyw 36

Tekst proponowany przez Komisję	*Poprawka*
(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	(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)***, 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

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.	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.

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 36

Wniosek dotyczący dyrektywy
Motyw 37

Tekst proponowany przez Komisję	*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 ***i*** opieki zdrowotnej.	(37) Przy stosowaniu niniejszej dyrektywy Komisja powinna w stosownych przypadkach współpracować z odpowiednimi komitetami sektorowymi i odpowiednimi organami ustanowionymi na poziomie ***Unii***, zwłaszcza w dziedzinie ***administracji elektronicznej,*** energetyki, transportu***,*** opieki zdrowotnej ***i obrony***.

Poprawka 37

Wniosek dotyczący dyrektywy
Motyw 38

Tekst proponowany przez Komisję	*Poprawka*
(38) Informacjami, które właściwy organ uznaje za poufne zgodnie z unijnymi i krajowymi przepisami dotyczącymi tajemnicy handlowej, można się wymieniać z Komisją ***i*** innymi właściwymi organami tylko wtedy, gdy wymiana taka jest absolutnie niezbędna w celu	(38) Informacjami, które właściwy organ ***lub pojedynczy punkt kontaktowy*** uznaje za poufne zgodnie z unijnymi i krajowymi przepisami dotyczącymi tajemnicy handlowej, można się wymieniać z Komisją, ***jej odpowiednimi agencjami,*** innymi ***pojedynczymi punktami***

wykonania niniejszej dyrektywy. Ujawnione informacje powinny ograniczać się do tego, co jest ***właściwe*** i proporcjonalne do celów takiej wymiany informacji.

kontaktowymi i/lub innymi właściwymi organami ***krajowymi*** tylko wtedy, gdy wymiana taka jest absolutnie niezbędna w celu wykonania niniejszej dyrektywy. Ujawnione informacje powinny ograniczać się do tego, co jest ***istotne, niezbędne*** i proporcjonalne do celów takiej wymiany informacji***, oraz być zgodne z ustalonymi wcześniej kryteriami poufności i bezpieczeństwa, na mocy decyzji Rady z dnia 31 marca 2011 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (2011/292/UE), do informacji objętych postanowieniami umów o zachowaniu poufności i nieformalnych umów o zachowaniu poufności, takich jak protokół TLP.***

Poprawka 38

Wniosek dotyczący dyrektywy
Motyw 39

Tekst proponowany przez Komisję	*Poprawka*
(39) Wymiana informacji dotyczących zagrożeń i incydentów w ramach sieci współpracy i zapewnienie zgodności z wymogami dotyczącymi zgłaszania incydentów właściwym organom krajowym mogą oznaczać konieczność przetwarzania danych osobowych. Takie przetwarzanie danych osobowych jest niezbędne do realizacji celów niniejszej dyrektywy będących w interesie publicznym i w związku z tym jest uzasadnione na mocy art. 7 dyrektywy 95/46/WE. Nie stanowi ono, w odniesieniu do tych uzasadnionych celów, nieproporcjonalnej i niedopuszczalnej ingerencji naruszającej istotę prawa do ochrony danych osobowych, które gwarantuje art. 8 Karty praw podstawowych Unii Europejskiej. Przy wdrażaniu niniejszej dyrektywy zastosowanie powinno mieć, w stosownych	(39) Wymiana informacji dotyczących zagrożeń i incydentów w ramach sieci współpracy i zapewnienie zgodności z wymogami dotyczącymi zgłaszania incydentów właściwym organom krajowym ***lub pojedynczym punktom kontaktowym*** mogą oznaczać konieczność przetwarzania danych osobowych. Takie przetwarzanie danych osobowych jest niezbędne do realizacji celów niniejszej dyrektywy będących w interesie publicznym i w związku z tym jest uzasadnione na mocy art. 7 dyrektywy 95/46/WE. Nie stanowi ono, w odniesieniu do tych uzasadnionych celów, nieproporcjonalnej i niedopuszczalnej ingerencji naruszającej istotę prawa do ochrony danych osobowych, które gwarantuje art. 8 Karty praw podstawowych Unii Europejskiej. Przy wdrażaniu niniejszej dyrektywy

przypadkach, rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji. W przypadku gdy dane są przetwarzane przez instytucje i organy Unii, tego rodzaju przetwarzanie w celu wprowadzenia niniejszej dyrektywy w życie powinno być zgodne z rozporządzeniem (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.

zastosowanie powinno mieć, w stosownych przypadkach, rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji. W przypadku gdy dane są przetwarzane przez instytucje i organy Unii, tego rodzaju przetwarzanie w celu wprowadzenia niniejszej dyrektywy w życie powinno być zgodne z rozporządzeniem (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.

Poprawka 39

Wniosek dotyczący dyrektywy
Motyw 41 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(41a) Zgodnie ze wspólną deklaracją polityczną państw członkowskich i Komisji dotyczącą dokumentów wyjaśniających z dnia 28 września 2011 r. państwa członkowskie zobowiązały się dołączać, w uzasadnionych przypadkach, do powiadomienia o środkach transpozycji jeden lub większą liczbę dokumentów wyjaśniających związki między elementami dyrektywy a odpowiadającymi im częściami krajowych instrumentów służących transpozycji. W odniesieniu do niniejszej dyrektywy ustawodawca uznaje, że przekazanie takich dokumentów jest uzasadnione.

Poprawka 40

Wniosek dotyczący dyrektywy
Artykuł 1 – ustęp 2 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) ustanawia mechanizm współpracy między państwami członkowskimi w celu zapewnienia jednolitego stosowania niniejszej dyrektywy w obrębie Unii oraz, w razie konieczności, w celu zapewnienia skoordynowanego ***i*** sprawnego postępowania w przypadku wystąpienia zagrożeń i incydentów dotyczących sieci i systemów informatycznych oraz reagowania na nie;	b) ustanawia mechanizm współpracy między państwami członkowskimi w celu zapewnienia jednolitego stosowania niniejszej dyrektywy w obrębie Unii oraz, w razie konieczności, w celu zapewnienia skoordynowanego***,*** sprawnego ***i skutecznego*** postępowania w przypadku wystąpienia zagrożeń i incydentów dotyczących sieci i systemów informatycznych oraz reagowania na nie***, z udziałem odpowiednich zainteresowanych stron***;

Poprawka 41

Wniosek dotyczący dyrektywy
Artykuł 1 – ustęp 2 – litera c

Tekst proponowany przez Komisję	*Poprawka*
c) ustanawia wymogi w zakresie bezpieczeństwa dla podmiotów gospodarczych ***i organów administracji publicznej***.	c) ustanawia wymogi w zakresie bezpieczeństwa dla podmiotów gospodarczych.

Poprawka 42

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	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.	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 ogranicza się do tego, co jest absolutnie niezbędne dla celów niniejszej dyrektywy, a dane te są anonimowe, jeśli nie zupełnie, to w jak największym stopniu.***

Poprawka 43

Wniosek dotyczący dyrektywy
Artykuł 1 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	Artykuł 1a
	Ochrona i przetwarzanie danych osobowych;
	1. Wszelkie przetwarzanie danych osobowych w państwach członkowskich na mocy niniejszej dyrektywy odbywa się zgodnie z dyrektywą 95/46/WE i dyrektywą 2002/58/WE.
	2. Wszelkie przetwarzanie danych osobowych przez Komisję i ENISA na mocy niniejszego rozporządzenia odbywa się zgodnie z rozporządzeniem (WE) nr 45/2001.

3. Wszelkie przetwarzanie danych osobowych przez działające przy Europolu Centrum ds. Walki z Cyberprzestępczością do celów niniejszej dyrektywy odbywa się na mocy decyzji 2009/371/WSiSW.

4. Przetwarzanie danych osobowych jest uczciwe i zgodne z prawem oraz ściśle ograniczone do minimalnych danych niezbędnych do celów, w których odbywa się ich przetwarzanie. Są one przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez czas nie dłuższy niż jest to konieczne do celów, w których dane osobowe są przetwarzane.

5. Zgłaszanie incydentów, o którym mowa w art. 14, pozostaje bez uszczerbku dla określonych w art. 4 dyrektywy 2002/58/WE i w rozporządzeniu (UE) nr 611/2013 przepisów i obowiązków dotyczących powiadamiania o przypadkach naruszenia danych osobowych.

Poprawka 44

Wniosek dotyczący dyrektywy
Artykuł 3 – punkt 1 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) wszelkie urządzenia lub grupy połączonych lub powiązanych urządzeń, z których jedno lub więcej, zgodnie z oprogramowaniem, dokonuje automatycznego przetwarzania danych ***komputerowych***, jak również	b) wszelkie urządzenia lub grupy połączonych lub powiązanych urządzeń, z których jedno lub więcej, zgodnie z oprogramowaniem, dokonuje automatycznego przetwarzania danych ***cyfrowych***, jak również

Poprawka 45

Wniosek dotyczący dyrektywy
Artykuł 3 – punkt 1 – litera c

Tekst proponowany przez Komisję	*Poprawka*
c) dane ***komputerowe*** przechowywane, przetwarzane, odzyskiwane lub przekazywane przez elementy określone w lit. a) i b) w celu ich eksploatacji, użycia, ochrony lub utrzymania;	c) dane ***cyfrowe*** przechowywane, przetwarzane, odzyskiwane lub przekazywane przez elementy określone w lit. a) i b) w celu ich eksploatacji, użycia, ochrony lub utrzymania;

Poprawka 46

Wniosek dotyczący dyrektywy
Artykuł 3 – punkt 2

Tekst proponowany przez Komisję	*Poprawka*
2) „bezpieczeństwo” oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na zdarzenia przypadkowe lub działania złośliwe naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przekazywanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy;	2) „bezpieczeństwo” oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na zdarzenia przypadkowe lub działania złośliwe naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przekazywanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy; ***„bezpieczeństwo” obejmuje odpowiednie urządzenia techniczne, rozwiązania i procedury operacyjne spełniające wymogi bezpieczeństwa określone w niniejszej dyrektywie.***

Poprawka 47

Wniosek dotyczący dyrektywy
Artykuł 3 – punkt 3

Tekst proponowany przez Komisję	*Poprawka*
3) „zagrożenie” oznacza każdą okoliczność lub zdarzenie, które mogą mieć niekorzystny wpływ na bezpieczeństwo;	3) „zagrożenie” oznacza każdą ***dającą się racjonalnie określić*** okoliczność lub zdarzenie, które mogą mieć niekorzystny wpływ na bezpieczeństwo;

Poprawka 48

Wniosek dotyczący dyrektywy
Artykuł 3 – punkt 4

Tekst proponowany przez Komisję	*Poprawka*
4) „incydent” oznacza ***każdą okoliczność lub*** zdarzenie, które ***mają*** rzeczywisty niekorzystny wpływ na bezpieczeństwo;	4) „incydent” oznacza ***każde*** zdarzenie, które ***ma*** rzeczywisty niekorzystny wpływ na bezpieczeństwo;

Poprawka 49

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***

Poprawka 50

Wniosek dotyczący dyrektywy
Artykuł 3 – punkt 7

Tekst proponowany przez Komisję	*Poprawka*
7) „postępowanie w przypadku incydentu” oznacza wszystkie procedury umożliwiające analizę i ograniczenie skutków ***incydentu*** oraz reakcję na niego;	7) „postępowanie w przypadku incydentu” oznacza wszystkie procedury umożliwiające ***wykrycie incydentu, zapobieżenie mu, jego*** analizę i ograniczenie ***jego*** skutków oraz reakcję na niego;

Poprawka 51

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***

Poprawka 52

Wniosek dotyczący dyrektywy
Artykuł 3 – punkt 8 – litera b

Tekst proponowany przez Komisję	*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**.**	b) operatora infrastruktury, która ma zasadnicze znaczenie dla utrzymania kluczowych działań gospodarczych i społecznych w dziedzinach energetyki, transportu, bankowości, ***infrastruktury rynków finansowych, internetowych punktów wymiany, łańcucha dostaw żywności*** i opieki zdrowotnej, ***a której uszkodzenie lub zniszczenie miałoby poważny wpływ na dane państwo członkowskie w postaci braku możliwości utrzymania tych funkcji (ich*** niewyczerpujący wykaz zamieszczony jest w załączniku II***), o ile dane sieci i systemy informatyczne są powiązane z jego podstawowymi usługami;***

Poprawka 53

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

Tekst proponowany przez Komisję	*Poprawka*
	8a) „incydent mający znaczące konsekwencje" oznacza incydent mający wpływ na bezpieczeństwo i ciągłość sieci informatycznej lub systemu informatycznego, który prowadzi do

poważnego zakłócenia istotnych funkcji gospodarczych lub społecznych;

Poprawka 54

Wniosek dotyczący dyrektywy
Artykuł 3 – punkt 11 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	11a) „rynek regulowany" oznacza rynek regulowany w rozumieniu art. 4 pkt 14 dyrektywy 2004/39/WE Parlamentu Europejskiego i Rady[1a];
	[1a] Dyrektywa 2004/39/WE Parlamentu Europejskiego i Rady z dnia 21 kwietnia 2004 r. w sprawie rynków instrumentów finansowych (Dz.U. L 45 z 16.2.2005, s. 18).

Uzasadnienie

Dostosowanie definicji do nieprzyjętego jeszcze rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynków instrumentów finansowych oraz zmieniającego rozporządzenie [EMIR] w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji.

Poprawka 55

Wniosek dotyczący dyrektywy
Artykuł 3 – punkt 11 b (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	11b) „wielostronna platforma obrotu (MTF)" oznacza wielostronną platformę obrotu w rozumieniu art. 4 pkt 15 dyrektywy 2004/39/WE;

Uzasadnienie

Dostosowanie definicji do nieprzyjętego jeszcze rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynków instrumentów finansowych oraz zmieniającego rozporządzenie [EMIR] w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem

regulowanym, kontrahentów centralnych i repozytoriów transakcji.

Poprawka 56

Wniosek dotyczący dyrektywy
Artykuł 3 – punkt 11 c (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	11c) „zorganizowana platforma obrotu" oznacza wielostronny system lub wielostronną platformę, niebędące rynkiem regulowanym, wielostronną platformą obrotu ani centralnym kontrahentem, obsługiwane przez przedsiębiorstwo inwestycyjne lub podmiot gospodarczy, w ramach których umożliwia się wzajemne powiązanie w obrębie systemu interesów licznych stron trzecich w zakresie kupna i sprzedaży obligacji, strukturyzowanych produktów finansowych, uprawnień do emisji lub instrumentów pochodnych w sposób skutkujący zawarciem kontraktu, zgodnie z tytułem II dyrektywy 2004/38/WE;

Uzasadnienie

Wprowadzenie definicji zgodnej z nieprzyjętym jeszcze rozporządzeniem Parlamentu Europejskiego i Rady w sprawie rynków instrumentów finansowych oraz zmieniającym rozporządzenie [EMIR] w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji.

Poprawka 57

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

Tekst proponowany przez Komisję	*Poprawka*
	ea) Państwa członkowskie mogą zwrócić się do ENISA o pomoc w opracowywaniu krajowych strategii w zakresie bezpieczeństwa sieci i informacji oraz krajowych planów współpracy w zakresie

bezpieczeństwa sieci i informacji na podstawie wspólnej minimalnej strategii w zakresie bezpieczeństwa sieci i informacji.

Poprawka 58

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***;

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 59

Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 2 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) określenie funkcji i zakresu obowiązków poszczególnych podmiotów zaangażowanych ***w realizację planu***;	b) określenie funkcji i zakresu obowiązków poszczególnych ***organów i innych*** podmiotów zaangażowanych ***we wdrażanie tych ram***;

Poprawka 60

Wniosek dotyczący dyrektywy

Artykuł 5 – ustęp 3

Tekst proponowany przez Komisję	*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 ***jednego miesiąca*** od ich przyjęcia.	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.

Poprawka 61

Wniosek dotyczący dyrektywy
Artykuł 6 – nagłówek

Tekst proponowany przez Komisję	*Poprawka*
Właściwy organ krajowy ds. bezpieczeństwa sieci i systemów informatycznych	***Właściwe organy krajowe i krajowe pojedyncze punkty kontaktowe*** ds. bezpieczeństwa sieci i systemów informatycznych

Poprawka 62

Wniosek dotyczący dyrektywy
Artykuł 6 – ustęp 1

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

Uzasadnienie

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

Poprawka 63

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.

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 64

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

Tekst proponowany przez Komisję	*Poprawka*
	2b. Właściwe organy i pojedynczy punkt kontaktowy tego samego państwa członkowskiego ściśle ze sobą współpracują w zakresie obowiązków określonych w niniejszej dyrektywie.

Poprawka 65

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

Tekst proponowany przez Komisję	*Poprawka*
	2c. Pojedynczy punkt kontaktowy zapewnia współpracę transgraniczną z innymi pojedynczymi punktami kontaktowymi.

Poprawka 66

Wniosek dotyczący dyrektywy
Artykuł 6 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Państwa członkowskie zapewniają właściwym organom odpowiednie zasoby techniczne, finansowe i ludzkie, aby mogły one skutecznie i efektywnie realizować powierzone im zadania w celu osiągnięcia celów niniejszej dyrektywy. Państwa członkowskie zapewniają skuteczną, efektywną i bezpieczną współpracę ***właściwych organów*** za pośrednictwem sieci, o której mowa w art. 8.	3. Państwa członkowskie zapewniają właściwym organom ***i pojedynczym punktom kontaktowym*** odpowiednie zasoby techniczne, finansowe i ludzkie, aby mogły one skutecznie i efektywnie realizować powierzone im zadania w celu osiągnięcia celów niniejszej dyrektywy. Państwa członkowskie zapewniają skuteczną, efektywną i bezpieczną współpracę ***pojedynczych punktów kontaktowych*** za pośrednictwem sieci, o której mowa w art. 8.

Poprawka 67

Wniosek dotyczący dyrektywy
Artykuł 6 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
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.	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.

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 68

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

Tekst proponowany przez Komisję	*Poprawka*
	4a. Jeżeli prawo Unii przewiduje 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 określonych w rozdziale III.

Poprawka 69

Wniosek dotyczący dyrektywy
Artykuł 6 – ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. W stosownych przypadkach właściwe	5. W stosownych przypadkach właściwe

organy konsultują się i współpracują z odpowiednimi krajowymi organami ścigania i z organami ochrony danych.	organy ***i pojedyncze punkty kontaktowe*** konsultują się i współpracują z odpowiednimi krajowymi organami ścigania i z organami ochrony danych.

Poprawka 70

Wniosek dotyczący dyrektywy
Artykuł 6 – ustęp 6

Tekst proponowany przez Komisję	*Poprawka*
6. Każde państwo członkowskie powiadamia niezwłocznie Komisję o wyznaczeniu ***właściwego organu***, o ***jego*** zadaniach i o wszelkich późniejszych zmianach ***dotyczących tego organu***. Każde państwo członkowskie podaje do publicznej wiadomości informację o wyznaczeniu ***swojego właściwego organu***.	6. Każde państwo członkowskie powiadamia niezwłocznie Komisję o wyznaczeniu ***właściwych organów i pojedynczego punktu kontaktowego***, o ***ich*** zadaniach i o ***dotyczących ich*** wszelkich późniejszych zmianach. Każde państwo członkowskie podaje do publicznej wiadomości informację o wyznaczeniu ***właściwych organów***.

Poprawka 71

Wniosek dotyczący dyrektywy
Artykuł 7 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Każde państwo członkowskie ustanawia zespół reagowania na incydenty komputerowe (zwany dalej „CERT”), odpowiedzialny za postępowanie w przypadku wystąpienia incydentów i zagrożeń według jasno określonej procedury, która jest zgodna z wymogami określonymi w załączniku I pkt 1. CERT może zostać ustanowiony w ramach właściwego organu.	1. Każde państwo członkowskie ustanawia ***przynajmniej jeden*** zespół reagowania na incydenty komputerowe (zwany dalej „CERT”) ***dla każdego sektora określonego w załączniku II***, odpowiedzialny za postępowanie w przypadku wystąpienia incydentów i zagrożeń według jasno określonej procedury, która jest zgodna z wymogami określonymi w załączniku I pkt 1. CERT może zostać ustanowiony w ramach właściwego organu.

Poprawka 72

Wniosek dotyczący dyrektywy
Artykuł 7 – ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. CERT ***działa*** pod nadzorem właściwego organu, który regularnie dokonuje przeglądu stosowności ***jego*** zasobów, ***jego mandatu*** oraz skuteczności ***jego*** procedury postępowania w przypadku incydentów.	5. CERT ***działają*** pod nadzorem właściwego organu ***lub pojedynczego punktu kontaktowego***, który regularnie dokonuje przeglądu stosowności ***ich*** zasobów, ***mandatów*** oraz skuteczności ***ich*** procedury postępowania w przypadku incydentów.

Poprawka 73

Wniosek dotyczący dyrektywy
Artykuł 7 – ustęp 5 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	5a. Państwa członkowskie zapewniają CERT odpowiednie zasoby ludzkie i finansowe, aby mogły one czynnie uczestniczyć w międzynarodowych, a zwłaszcza unijnych, sieciach współpracy.

Poprawka 74

Wniosek dotyczący dyrektywy
Artykuł 7 – ustęp 5 b (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	5b. CERT są uprawnione i zachęcane do inicjowania wspólnych ćwiczeń z innymi CERT, z CERT ze wszystkich państw członkowskich oraz z właściwymi instytucjami państw trzecich, a także z CERT instytucji wielonarodowych i międzynarodowych, takich jak NATO czy ONZ, oraz do udziału w takich wspólnych

ćwiczeniach.

Poprawka 75

Wniosek dotyczący dyrektywy
Artykuł 7 – ustęp 5 c (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	5c. Państwa członkowskie mogą zwrócić się do ENISA lub do innych państw członkowskich o pomoc w rozwijaniu krajowych CERT.

Poprawka 76

Wniosek dotyczący dyrektywy
Artykuł 8 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. ***Właściwe organy i*** Komisja ustanawiają sieć („***sieć*** współpracy") służącą do współpracy w zakresie przeciwdziałania zagrożeniom i incydentom dotyczącym sieci i systemów informatycznych.	1. ***Pojedyncze punkty kontaktowe,*** Komisja ***i ENISA*** ustanawiają sieć (***zwaną dalej*** „***siecią*** współpracy") służącą do współpracy w zakresie przeciwdziałania zagrożeniom i incydentom dotyczącym sieci i systemów informatycznych.

Poprawka 77

Wniosek dotyczący dyrektywy
Artykuł 8 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
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.	2. Sieć współpracy umożliwia stałą łączność między Komisją a ***pojedynczymi punktami kontaktowymi***. ***ENISA wspiera,*** na żądanie***,*** 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) oraz i).
	W stosownych przypadkach sieć współpracy współpracuje z organami ochrony danych.
	Komisja regularnie informuje sieć współpracy o badaniach dotyczących bezpieczeństwa oraz innych stosownych programach programu „Horyzont 2020”.

Poprawka 78

Wniosek dotyczący dyrektywy
Artykuł 8 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. W ramach sieci współpracy ***właściwe organy***:	3. W ramach sieci współpracy ***pojedyncze punkty kontaktowe***:
a) przekazują wczesne ostrzeżenia dotyczące zagrożeń i incydentów zgodnie z art. 10;	a) przekazują wczesne ostrzeżenia dotyczące zagrożeń i incydentów zgodnie z art. 10;
b) zapewniają skoordynowaną reakcję zgodnie z art. 11;	b) zapewniają skoordynowaną reakcję zgodnie z art. 11;
c) regularnie publikują na wspólnej stronie internetowej niemające poufnego charakteru informacje na temat aktualnych wczesnych ostrzeżeń i skoordynowanych reakcji;	c) regularnie publikują na wspólnej stronie internetowej niemające poufnego charakteru informacje na temat aktualnych wczesnych ostrzeżeń i skoordynowanych reakcji;
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;	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;
e) wspólnie omawiają i oceniają***, na wniosek państwa członkowskiego lub Komisji,*** skuteczność CERT, zwłaszcza w przypadku gdy ćwiczenia w zakresie bezpieczeństwa sieci i informacji	e) wspólnie omawiają i oceniają skuteczność CERT, zwłaszcza w przypadku gdy ćwiczenia w zakresie bezpieczeństwa sieci i informacji

przeprowadzane są na poziomie unijnym;

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***;

g) wymieniają się informacjami i najlepszymi praktykami między sobą i z Komisją oraz udzielają sobie wzajemnie pomocy w budowaniu zdolności w zakresie bezpieczeństwa sieci i informacji;

h) regularnie organizują wzajemne oceny zdolności i gotowości;

i) organizują ćwiczenia w zakresie bezpieczeństwa sieci i informacji na poziomie unijnym oraz uczestniczą, w stosownych przypadkach, w międzynarodowych ćwiczeniach w zakresie bezpieczeństwa sieci i informacji.

przeprowadzane są na poziomie unijnym;

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;

fa) w stosownych przypadkach przekazują w drodze sprawozdań informacje koordynatorowi UE ds. zwalczania terroryzmu i mogą zwrócić się o pomoc związaną z analizą, pracami przygotowawczymi i działaniami sieci współpracy;

g) wymieniają się informacjami i najlepszymi praktykami między sobą i z Komisją oraz udzielają sobie wzajemnie pomocy w budowaniu zdolności w zakresie bezpieczeństwa sieci i informacji;

i) organizują ćwiczenia w zakresie bezpieczeństwa sieci i informacji na poziomie unijnym oraz uczestniczą, w stosownych przypadkach, w międzynarodowych ćwiczeniach w zakresie bezpieczeństwa sieci i informacji.

ia) angażują podmioty gospodarcze, konsultują się z nimi i wymieniają się z nimi informacjami na temat zagrożeń i incydentów mających wpływ na ich sieci i systemy informatyczne;

ib) 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 w celu wspólnej wykładni, spójnego stosowania i harmonijnego wdrażania w Unii.

Poprawka 79

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

Tekst proponowany przez Komisję	*Poprawka*
	3a. Sieć współpracy publikuje raz w roku sprawozdanie za poprzednie 12 miesięcy oparte na działalności sieci i na sprawozdaniu podsumowującym przekazanym zgodnie z art. 14 ust. 4 niniejszej dyrektywy.

Poprawka 80

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, o której mowa w ust. 2 i 3***, pomiędzy pojedynczymi punktami kontaktowymi, Komisją i ENISA***. Te akty wykonawcze przyjmuje się zgodnie z procedurą ***sprawdzającą***, o której mowa w art. 19 ust. ***3***.

Poprawka 81

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

Tekst proponowany przez Komisję	*Poprawka*
	1a. Uczestnicy bezpiecznej infrastruktury spełniają m.in. odpowiednie wymogi poufności i bezpieczeństwa zgodnie z dyrektywą 95/46/WE i rozporządzeniem (WE) nr 45/2001 na każdym etapie przetwarzania.

Poprawka 82

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.	

Poprawka 83

Wniosek dotyczący dyrektywy
Artykuł 9 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
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.***	3. Komisja przyjmuje – w drodze aktów ***delegowanych – wspólny zestaw norm w zakresie wzajemnych połączeń i bezpieczeństwa, do*** których ***pojedyncze punkty kontaktowe mają się stosować przed wymianą szczególnie chronionych i poufnych informacji w ramach sieci współpracy.***

Poprawka 84

Wniosek dotyczący dyrektywy
Artykuł 10 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. W ramach sieci współpracy ***właściwe organy*** lub Komisja wydają wczesne ostrzeżenia dotyczące zagrożeń i incydentów, które spełniają co najmniej jeden z następujących warunków:	1. W ramach sieci współpracy ***pojedyncze punkty kontaktowe*** lub Komisja wydają wczesne ostrzeżenia dotyczące zagrożeń i incydentów, które spełniają co najmniej jeden z następujących warunków:
a) ich skala szybko rośnie lub może szybko wzrosnąć;	
b) ***przekraczają one lub mogą przekroczyć*** krajowe zdolności reagowania;	b) ***w ocenie pojedynczego punktu kontaktowego dane zagrożenie lub incydent potencjalnie przekracza*** krajowe zdolności reagowania;
c) ***mają one*** wpływ ***lub mogą mieć wpływ*** na więcej niż jedno państwo członkowskie.	c) ***w ocenie pojedynczego punktu kontaktowego lub Komisji dane zagrożenie lub incydent ma*** wpływ na więcej niż jedno państwo członkowskie.

Poprawka 85

Wniosek dotyczący dyrektywy
Artykuł 10 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Wraz z wczesnym ostrzeżeniem ***właściwe organy*** i Komisja przekazują wszelkie stosowne informacje będące w ich posiadaniu, które mogą być przydatne do oceny zagrożenia lub incydentu.	2. Wraz z wczesnym ostrzeżeniem ***pojedyncze punkty kontaktowe*** i Komisja przekazują ***bez zbędnej zwłoki*** wszelkie stosowne informacje będące w ich posiadaniu, które mogą być przydatne do oceny zagrożenia lub incydentu.

Poprawka 86

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***

Poprawka 87

Wniosek dotyczący dyrektywy
Artykuł 10 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
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.	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 dopilnowują, aby – w stosownych przypadkach – poinformowano o tym*** działające przy Europolu Europejskie Centrum ds. Walki z Cyberprzestępczością.

Poprawka 88

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, o których mowa w 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.

Poprawka 89

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

Tekst proponowany przez Komisję	*Poprawka*
	4b. W sytuacji gdy zachodzi podejrzenie, iż zagrożenie lub incydent będące przedmiotem wczesnego ostrzeżenia stanowią poważne zagrożenie lub poważny incydent o charakterze technicznym transnarodowym, pojedyncze punkty kontaktowe lub Komisja powiadamiają ENISA.

Poprawka 90

Wniosek dotyczący dyrektywy
Artykuł 11 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Po otrzymaniu wczesnego ostrzeżenia, o którym mowa w art. 10, ***właściwe organy*** – po przeanalizowaniu właściwych informacji – uzgadniają skoordynowaną reakcję zgodnie z unijnym planem współpracy w zakresie bezpieczeństwa sieci i informacji, o którym mowa w art. 12.	1. Po otrzymaniu wczesnego ostrzeżenia, o którym mowa w art. 10, ***pojedyncze punkty kontaktowe*** – po przeanalizowaniu właściwych informacji – uzgadniają ***bez zbędnej zwłoki*** skoordynowaną reakcję zgodnie z unijnym planem współpracy w zakresie bezpieczeństwa sieci i informacji, o którym mowa w art. 12.

Poprawka 91

Wniosek dotyczący dyrektywy
Artykuł 12 – ustęp 2 – litera a – tiret pierwsze

Tekst proponowany przez Komisję	*Poprawka*
– określenie formatu i procedur gromadzenia i wymiany kompatybilnych i porównywalnych informacji na temat zagrożeń i incydentów przez ***właściwe organy***;	– określenie formatu i procedur gromadzenia i wymiany kompatybilnych i porównywalnych informacji na temat zagrożeń i incydentów przez ***pojedyncze punkty kontaktowe***;

Poprawka 92

Wniosek dotyczący dyrektywy
Artykuł 12 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Unijny plan współpracy w zakresie bezpieczeństwa sieci i informacji przyjmuje się nie później niż jeden rok po wejściu w życie niniejszej dyrektywy i regularnie poddaje się go przeglądowi.	3. Unijny plan współpracy w zakresie bezpieczeństwa sieci i informacji przyjmuje się nie później niż jeden rok po wejściu w życie niniejszej dyrektywy i regularnie poddaje się go przeglądowi. ***Wyniki każdego przeglądu są przekazywane Parlamentowi Europejskiemu.***

Poprawka 93

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

Tekst proponowany przez Komisję	*Poprawka*
	3a. Należy zagwarantować spójność między unijnym planem współpracy w zakresie bezpieczeństwa sieci i informacji a krajowymi strategiami w zakresie bezpieczeństwa sieci i informacji i krajowymi planami współpracy w zakresie bezpieczeństwa sieci i informacji zgodnie z art. 5 niniejszej dyrektywy.

Poprawka 94

Wniosek dotyczący dyrektywy
Artykuł 13 – ustęp 1

Tekst proponowany przez Komisję	*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.	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 ***przekazywanych*** w ramach sieci współpracy ***i określają procedurę monitorowania, którą należy stosować, aby zagwarantować ochronę takich danych osobowych***. ***Parlament Europejski jest informowany o negocjacjach w sprawie tych umów. Każde przekazanie danych osobowych odbiorcom z siedzibą w krajach poza Unią odbywa się z zgodnie z art. 25 i 26 dyrektywy 95/46/WE oraz z art. 9 rozporządzenia (WE) nr 45/2001.***

Poprawka 95

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 którego upływie brak ciągłości świadczenia usług podstawowych przez podmiot gospodarczy ma negatywny wpływ na utrzymanie kluczowych działań gospodarczych i społecznych.

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 96

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 1

Tekst proponowany przez Komisję	*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. ***Uwzględniając aktualny stan*** wiedzy i technologii***, środki te zapewniają poziom bezpieczeństwa stosowny do istniejącego zagrożenia***. W szczególności należy ***podjąć*** środki zapobiegające incydentom ***dotyczącym*** sieci i systemów informatycznych ***organów administracji publicznej i podmiotów gospodarczych*** oraz minimalizujące wpływ tych incydentów na świadczone przez nie podstawowe usługi, zapewniając tym	1. Państwa członkowskie zapewniają zastosowanie przez podmioty gospodarcze właściwych ***i proporcjonalnych*** środków technicznych i organizacyjnych w celu ***wykrywania zagrożeń***, na jakie narażone są kontrolowane i wykorzystywane przez nie sieci i systemy informatyczne***, oraz skutecznego przeciwdziałania im***. ***Środki te gwarantują poziom bezpieczeństwa proporcjonalny do istniejącego ryzyka z uwzględnieniem aktualnego stanu*** wiedzy i technologii. W szczególności należy ***przyjąć*** środki zapobiegające incydentom ***mającym wpływ na bezpieczeństwo ich*** sieci i systemów informatycznych oraz minimalizujące wpływ tych incydentów na świadczone przez nie podstawowe usługi, zapewniając tym samym ciągłość usług opartych na tych sieciach i systemach

samym ciągłość usług opartych na tych sieciach i systemach informatycznych.	informatycznych.

Poprawka 97

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Państwa członkowskie dopilnowują, aby ***organy administracji publicznej oraz*** podmioty gospodarcze zgłaszały ***właściwym organom*** incydenty mające znaczące konsekwencje dla ***bezpieczeństwa*** świadczonych przez nie usług podstawowych.	2. Państwa członkowskie dopilnowują, aby podmioty gospodarcze ***niezwłocznie*** zgłaszały ***właściwemu organowi lub pojedynczemu punktowi kontaktowemu*** incydenty mające znaczące konsekwencje dla ***ciągłości*** świadczonych przez nie usług podstawowych. ***Zgłoszenie nie może narażać strony zgłaszającej na większą odpowiedzialność.*** ***Aby określić znaczenie konsekwencji danego incydentu, uwzględnia się m.in. następujące parametry:***

Poprawka 98

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 2 – litera a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	a) liczbę użytkowników korzystających z usługi podstawowej, na którą ma wpływ dany incydent;

Poprawka 99

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 2 – litera b (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	b) czas trwania incydentu;

Poprawka 100

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 2 – litera c (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	c) zasięg geograficzny związany z obszarem, którego dotyczy incydent.

Poprawka 101

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).

Poprawka 102

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

Tekst proponowany przez Komisję	*Poprawka*
	2a. Podmioty gospodarcze zgłaszają incydenty, o których mowa w ust. 1 i 2, właściwemu organowi lub pojedynczemu punktowi kontaktowemu w państwie członkowskim, w którym incydent ma wpływ na podstawową usługę. Jeżeli incydent ma wpływ na usługi podstawowe w więcej niż jednym państwie członkowskim, pojedynczy punkt kontaktowy, który otrzymał zgłoszenie, alarmuje pozostałe zainteresowane pojedyncze punkty kontaktowe, opierając się na informacjach dostarczonych przez dany podmiot gospodarczy. Podmiotowi gospodarczemu przekazuje się w możliwie najkrótszym terminie informacje na temat innych pojedynczych punktów kontaktowych powiadomionych o incydencie, a także wszelkich podjętych

kroków, rezultatów oraz wszelkie inne informacje mające znaczenie dla incydentu.

Poprawka 103

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

Tekst proponowany przez Komisję	*Poprawka*
	2b. Jeżeli zgłoszenie zawiera dane osobowe, jest ono ujawniane wyłącznie odbiorcom powiadomionego właściwego organu lub pojedynczego punktu kontaktowego, którzy muszą przetwarzać te dane w ramach swoich obowiązków zgodnie z przepisami dotyczącymi ochrony danych. Zakres ujawnianych danych ogranicza się do tego, co niezbędne do wykonywania tych zadań.

Poprawka 104

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

Tekst proponowany przez Komisję	*Poprawka*
	2c. Podmioty gospodarcze nieobjęte załącznikiem II mogą zgłaszać incydenty określone w art. 14 ust. 2 na zasadzie dobrowolności.

Poprawka 105

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
4. ***W przypadku gdy właściwy organ uznaje***, że ***ujawnienie incydentu leży w interesie publicznym, może on podać informację o incydencie do wiadomości***	4. ***Po konsultacji z powiadomionym właściwym organem i zainteresowanym podmiotem gospodarczym pojedynczy punkt kontaktowy może poinformować***

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.	***opinię publiczną o pojedynczych incydentach, jeżeli uzna,*** że ***wiedza obywateli na ten temat jest niezbędna, by zapobiec incydentowi bądź uporać się z bieżącym incydentem, lub jeżeli podmiot gospodarczy, którego dotyczy incydent, odmówił niezwłocznego usunięcia poważnej strukturalnej usterki związanej z tym incydentem.*** ***Przed podaniem informacji o incydencie do wiadomości publicznej powiadomiony właściwy organ dopilnowuje, aby zainteresowany podmiot gospodarczy miał możliwość wypowiedzenia się oraz aby decyzja o upublicznieniu takich informacji była należycie wyważona w odniesieniu do interesu publicznego.*** ***W przypadku podania informacji o pojedynczych incydentach do wiadomości publicznej powiadomiony właściwy organ lub pojedynczy punkt kontaktowy dopilnowuje, aby odbyło się to jak najbardziej anonimowo.*** ***Właściwy organ lub pojedynczy punkt kontaktowy udziela, w miarę możliwości, zainteresowanemu podmiotowi gospodarczemu informacji pomocnych w skutecznym rozwiązaniu zgłoszonego incydentu.***
Raz do roku ***właściwy organ*** przekazuje sieci współpracy sprawozdanie podsumowujące otrzymane zgłoszenia ***i działania*** podjęte zgodnie z niniejszym ustępem.	Raz do roku ***pojedynczy punkt kontaktowy*** przekazuje sieci współpracy sprawozdanie podsumowujące otrzymane zgłoszenia***, w tym informacje o liczbie zgłoszeń i parametrach incydentu wyszczególnionych w ust. 2 niniejszego artykułu, oraz działania*** podjęte zgodnie z niniejszym ustępem.

Poprawka 106

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

Tekst proponowany przez Komisję	*Poprawka*
	4a. Państwa członkowskie powinny zachęcać podmioty gospodarcze, aby na zasadzie dobrowolności informowały opinię publiczną w swoich sprawozdaniach finansowych o incydentach związanych ze swoją działalnością.

Poprawka 107

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. Komisja jest uprawniona do przyjęcia aktów delegowanych zgodnie z art. 18 dotyczących określenia okoliczności, w których organy administracji publicznej i podmioty gospodarcze są zobowiązane do zgłaszania incydentów.	***skreślony***

Poprawka 108

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 6

Tekst proponowany przez Komisję	*Poprawka*
6. ***Z zastrzeżeniem wszelkich aktów delegowanych przyjętych na mocy ust. 5,*** właściwe organy mogą przyjąć wytyczne***, a w razie konieczności wydać instrukcje*** dotyczące okoliczności, w których ***organy administracji publicznej i*** podmioty gospodarcze są zobowiązane do zgłaszania incydentów.	6. Właściwe organy ***lub pojedyncze punkty kontaktowe*** mogą przyjąć wytyczne dotyczące okoliczności, w których podmioty gospodarcze są zobowiązane do zgłaszania incydentów.

Poprawka 109

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 8

Tekst proponowany przez Komisję	*Poprawka*
8. Ustępów 1 i 2 nie stosuje się w odniesieniu do mikroprzedsiębiorstw określonych w zaleceniu Komisji 2003/361/WE z dnia 6 maja 2003 r. w sprawie definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw[35].	8. Ustępów 1 i 2 nie stosuje się w odniesieniu do mikroprzedsiębiorstw określonych w zaleceniu Komisji 2003/361/WE z dnia 6 maja 2003 r. w sprawie definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw[35]***, chyba że mikroprzedsiębiorstwo działa jako jednostka zależna podmiotu gospodarczego, o którym mowa w art. 3 pkt 8 lit. b).***
[35] Dz.U. L 124 z 20.5.2003, s. 36.	[35] Dz.U. L 124 z 20.5.2003, s. 36.

Poprawka 110

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.

Poprawka 111

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Państwa członkowskie zapewniają właściwym organom ***wszelkie*** uprawnienia niezbędne do ***badania przypadków niewypełniania przez organy administracji publicznej lub podmioty gospodarcze zobowiązań ciążących*** na nich na mocy art. 14 oraz ich wpływu na bezpieczeństwo sieci i systemów informatycznych.	1. Państwa członkowskie zapewniają właściwym organom ***i pojedynczym punktom kontaktowym*** uprawnienia niezbędne do ***zapewnienia zgodności ze zobowiązaniami ciążącymi*** na nich na mocy art. 14 oraz ich wpływu na bezpieczeństwo sieci i systemów informatycznych.

Poprawka 112

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 2 – wprowadzenie

Tekst proponowany przez Komisję	*Poprawka*
2. Państwa członkowskie zapewniają właściwym organom uprawnienia, na podstawie których mogą one wymagać od podmiotów gospodarczych ***i organów administracji publicznej***:	2. Państwa członkowskie zapewniają właściwym organom ***i pojedynczym punktom kontaktowym*** uprawnienia, na podstawie których mogą one wymagać od podmiotów gospodarczych:

Poprawka 113

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 2 – litera b

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

Poprawka 114

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 2 – akapit pierwszy a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	Kierując taki wniosek, właściwe organy i pojedyncze punkty kontaktowe podają cel wniosku i określają dokładnie, jakie informacje są wymagane.

Poprawka 115

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Państwa członkowskie zapewniają właściwym organom uprawnienia do wydawania wiążących instrukcji dla podmiotów gospodarczych ***i organów administracji publicznej***.	3. Państwa członkowskie zapewniają właściwym organom ***i pojedynczym punktom kontaktowym*** uprawnienia do wydawania wiążących instrukcji dla podmiotów gospodarczych.

Poprawka 116

Wniosek dotyczący dyrektywy
Artykuł 15 – ustępy 3 a i 3 b (nowe)

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.

3b. Państwa członkowskie mogą podjąć decyzję o zmniejszeniu liczby i intensywności audytów w odniesieniu do danego podmiotu gospodarczego, jeśli przeprowadzony w nim audyt bezpieczeństwa wykazał konsekwentną zgodność z postanowieniami rozdziału IV.

Poprawka 117

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
4. Właściwe organy ***zgłaszają*** organom ścigania ***poważne incydenty, które mogą mieć charakter przestępczy***.	4. Właściwe organy ***i pojedyncze punkty kontaktowe informują zainteresowane podmioty gospodarcze o możliwości zgłaszania*** organom ścigania ***incydentów noszących znamiona poważnego przestępstwa***.

Poprawka 118

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. W przypadku incydentów prowadzących do ***naruszeń*** danych osobowych właściwe organy działają w ścisłej współpracy z organami ochrony danych osobowych.	5. ***Bez uszczerbku dla obowiązującego prawa o ochronie danych,*** w przypadku incydentów prowadzących do ***naruszenia przepisów o ochronie*** danych osobowych właściwe organy ***i pojedyncze punkty kontaktowe*** działają w ścisłej współpracy z organami ochrony danych osobowych. ***Pojedyncze punkty kontaktowe i organy ochrony danych opracowują we współpracy z ENISA mechanizmy wymiany informacji oraz jednolity wzór formularza wykorzystywanego zarówno w przypadku zgłoszeń na podstawie art. 14***

	ust. 2 niniejszej dyrektywy, jak i na podstawie prawa Unii o ochronie danych.

Poprawka 119

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 6

Tekst proponowany przez Komisję	*Poprawka*
6. Państwa członkowskie zapewniają możliwość poddania kontroli sądowej wszelkich obowiązków nałożonych na ***organy administracji publicznej oraz*** podmioty gospodarcze na mocy niniejszego rozdziału.	6. Państwa członkowskie zapewniają możliwość poddania kontroli sądowej wszelkich obowiązków nałożonych na podmioty gospodarcze na mocy niniejszego rozdziału.

Poprawka 120

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.

Poprawka 121

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***, nie nakazując stosowania żadnej konkretnej technologii,*** wspierają stosowanie ***europejskich lub międzynarodowych interoperacyjnych*** norm lub specyfikacji mających znaczenie dla bezpieczeństwa sieci i informacji.

Poprawka 122

Wniosek dotyczący dyrektywy
Artykuł 16 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Komisja ***sporządza – w drodze aktów wykonawczych – wykaz*** norm, o których mowa w ust. 1. Wykaz ten zostaje opublikowany w Dzienniku Urzędowym Unii Europejskiej.	2. Komisja ***nadaje odpowiedniemu organowi normalizacji europejskiej mandat do sporządzenia, w konsultacji z odpowiednimi zainteresowanymi stronami, wykazu*** norm ***lub specyfikacji***, o których mowa w ust. 1. Wykaz ten zostaje opublikowany w Dzienniku Urzędowym Unii Europejskiej.

Poprawka 123

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.

Poprawka 124

Wniosek dotyczący dyrektywy
Artykuł 18 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Przekazanie ***uprawnień***, o którym mowa w art. 9 ust. 2, ***art. 10 ust. 5 i art. 14 ust. 5,*** może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna od	3. Przekazanie ***uprawnienia,*** o którym mowa w art. 9 ust. 2, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna od

następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej lub w określonym w tej decyzji późniejszym terminie. Nie wpływa ona na ważność jakichkolwiek już obowiązujących aktów delegowanych.	następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w określonym w tej decyzji późniejszym terminie. Nie wpływa ona na ważność jakichkolwiek już obowiązujących aktów delegowanych.

Poprawka 125

Wniosek dotyczący dyrektywy
Artykuł 18 – ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. Akt delegowany przyjęty na podstawie art. 9 ust. 2, ***art. 10 ust. 5 i art. 14 ust. 5*** wchodzi w życie tylko ***wówczas, gdy*** Parlament Europejski albo Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie**,** lub ***gdy,*** przed upływem tego terminu**,** zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.	5. Akt delegowany przyjęty na podstawie art. 9 ust. 2 wchodzi w życie tylko ***wtedy***, ***kiedy*** Parlament Europejski albo Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie lub ***kiedy*** przed upływem tego terminu zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

Poprawka 126

Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
Komisja dokonuje okresowego przeglądu funkcjonowania niniejszej dyrektywy i składa Parlamentowi Europejskiemu i Radzie sprawozdania na ten temat. Pierwsze sprawozdanie należy przedłożyć nie później niż trzy lata po dacie transpozycji, o której mowa w art. 21. W tym celu Komisja może zwrócić się do państw członkowskich o bezzwłoczne dostarczenie informacji.	Komisja dokonuje okresowego przeglądu funkcjonowania niniejszej dyrektywy***, w szczególności wykazu zawartego w załączniku II,*** i składa Parlamentowi Europejskiemu i Radzie sprawozdania na ten temat. Pierwsze sprawozdanie należy przedłożyć nie później niż trzy lata po dacie transpozycji, o której mowa w art. 21. W tym celu Komisja może zwrócić się do państw członkowskich o bezzwłoczne

dostarczenie informacji.

Poprawka 127

Wniosek dotyczący dyrektywy
Załącznik 1 – nagłówek 1

Tekst proponowany przez Komisję	*Poprawka*
Zespoły reagowania na incydenty komputerowe (CERT) **– *wymogi i zadania***	***Wymogi i zadania zespołów*** reagowania na incydenty komputerowe (CERT)

Poprawka 128

Wniosek dotyczący dyrektywy
Artykuł 1 – ustęp 1 – punkt 1 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) CERT ***zapewnia*** wysoką dostępność swoich usług łączności poprzez unikanie pojedynczych punktów awarii oraz ***dysponuje*** różnymi kanałami, za pomocą których można się z ***nim*** skontaktować i za pomocą których ***on sam może*** się kontaktować z innymi. Ponadto kanały komunikacyjne są wyraźnie określone i dobrze znane wśród użytkowników CERT i wśród współpracujących partnerów.	a) CERT ***zapewniają*** wysoką dostępność swoich usług łączności poprzez unikanie pojedynczych punktów awarii oraz ***dysponują*** różnymi kanałami, za pomocą których ***zawsze*** można się z ***nimi*** skontaktować i za pomocą których ***one same mogą*** się kontaktować z innymi. Ponadto kanały komunikacyjne są wyraźnie określone i dobrze znane wśród użytkowników CERT i wśród współpracujących partnerów.

Poprawka 129

Wniosek dotyczący dyrektywy
Artykuł 1 – ustęp 1 – punkt 1 – litera c

Tekst proponowany przez Komisję	*Poprawka*
c) Biura CERT oraz wspierające systemy informatyczne są zlokalizowane w bezpiecznych miejscach.	c) Biura CERT oraz wspierające systemy informatyczne są zlokalizowane w bezpiecznych miejscach ***z zabezpieczonymi***

sieciowymi systemami informatycznymi.

Poprawka 130

Wniosek dotyczący dyrektywy
Artykuł 1 – ustęp 1 – punkt 2 – litera a – tiret pierwsze

Tekst proponowany przez Komisję	*Poprawka*
– monitorowanie incydentów na poziomie krajowym;	– ***wykrywanie i*** monitorowanie incydentów na poziomie krajowym;

Poprawka 131

Wniosek dotyczący dyrektywy
Załącznik I – punkt 2 – litera a – tiret piąte a (nowe)

Tekst proponowany przez Komisję	*Poprawka*
	– czynny udział w unijnych i międzynarodowych sieciach współpracy CERT;

Poprawka 132

Wniosek dotyczący dyrektywy
Załącznik II – wprowadzenie

Tekst proponowany przez Komisję	*Poprawka*
Wykaz podmiotów gospodarczych	Wykaz podmiotów gospodarczych
o których mowa w art. 3 ust. 8 lit. a):	
1. platformy handlu elektronicznego	
2. internetowe portale płatnicze	
3. portale społecznościowe	
4. wyszukiwarki	
5. usługi chmur obliczeniowych	

6. sklepy z aplikacjami

o których mowa w art. 3 ust. 8 lit. b):

Poprawka 133

Wniosek dotyczący dyrektywy
Załącznik II – punkt 1

Tekst proponowany przez Komisję	*Poprawka*
Wykaz podmiotów gospodarczych	Wykaz podmiotów gospodarczych
1. Energetyka	1. Energetyka
	a) Energia elektryczna
– dostawcy energii elektrycznej i gazu	***– dostawcy***
– operatorzy systemów dystrybucyjnych energii elektrycznej lub gazu oraz detaliści sprzedający energię elektryczną lub gaz konsumentom końcowym	***– operatorzy systemów dystrybucyjnych oraz detaliści sprzedający energię elektryczną konsumentom końcowym***
– operatorzy systemów przesyłowych gazu ziemnego, operatorzy systemu magazynowania i operatorzy systemów LNG	
– operatorzy systemów przesyłowych energii elektrycznej	***– operatorzy systemów przesyłowych energii elektrycznej***
	b) Ropa naftowa
– podmioty eksploatujące rurociągi przesyłowe i magazyny ropy naftowej	***– podmioty eksploatujące rurociągi przesyłowe i magazyny ropy naftowej***
	– operatorzy instalacji służących do produkcji, rafinacji, przetwarzania, magazynowania i przesyłu ropy naftowej
	c) Gaz
– podmioty działające na rynku gazu i energii elektrycznej	***– dostawcy***
	– operatorzy systemów dystrybucyjnych oraz detaliści sprzedający gaz konsumentom końcowym
	– operatorzy systemów przesyłowych gazu ziemnego, operatorzy systemu magazynowania i operatorzy systemów LNG
– operatorzy instalacji służących do	***– operatorzy instalacji służących do***

produkcji ropy naftowej i gazu ziemnego, obiekty służące do rafinacji i przetwarzania	***produkcji, rafinacji, przetwarzania, magazynowania i przesyłu gazu ziemnego***
	– podmioty działające na rynku gazu

Poprawka 134

Wniosek dotyczący dyrektywy
Załącznik II – punkt 2

Tekst proponowany przez Komisję	*Poprawka*
2. Transport	***2. Transport***
– przewoźnicy lotniczy (przewozy pasażerskie i towarowe)	***a) Transport drogowy***
– przewoźnicy morscy (przedsiębiorstwa świadczące usługi pasażerskiego transportu morskiego i przybrzeżnego oraz przedsiębiorstwa świadczące usługi towarowego transportu morskiego i przybrzeżnego)	***(i) operatorzy zarządzający ruchem***
– koleje (zarządcy infrastruktury, przedsiębiorstwa zintegrowane oraz przedsiębiorstwa transportu kolejowego)	***(ii) pomocnicze usługi logistyczne:***
– porty lotnicze	***– magazynowanie i składowanie***
– porty	***– przeładunek oraz***
– operatorzy zarządzający ruchem	***– pozostała działalność wspomagająca transport***
– pomocnicze usługi logistyczne: a) magazynowanie oraz składowanie, b) przeładunek i c) pozostała działalność wspomagająca transport	***b) Transport kolejowy***
	(i) koleje (zarządcy infrastruktury, przedsiębiorstwa zintegrowane oraz przedsiębiorstwa transportu kolejowego)
	(ii) operatorzy zarządzający ruchem
	(iii) pomocnicze usługi logistyczne:
	– magazynowanie i składowanie
	– przeładunek oraz
	– pozostała działalność wspomagająca

	transport
	c) Transport lotniczy
	(i) przewoźnicy lotniczy (przewozy pasażerskie i towarowe)
	(ii) porty lotnicze
	(iii) operatorzy zarządzający ruchem
	(iv) pomocnicze usługi logistyczne:
	– magazynowanie
	– przeładunek oraz
	– pozostała działalność wspomagająca transport
	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)

Poprawka 135

Wniosek dotyczący dyrektywy
Załącznik II – punkt 4

Tekst proponowany przez Komisję	*Poprawka*
4. Infrastruktura rynków finansowych: giełdy papierów wartościowych i izby rozliczeniowe partnerów centralnych	***4. Infrastruktura rynków finansowych: rynki regulowane, wielostronne platformy obrotu, zorganizowane platformy obrotu i izby rozliczeniowe kontrahentów centralnych***

Poprawka 136

Wniosek dotyczący dyrektywy
Załącznik II – punkt 5a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	5a. Produkcja wody i zaopatrzenie w wodę

Poprawka 137

Wniosek dotyczący dyrektywy
Załącznik II – punkt 5 b (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	5b. Łańcuch dostaw żywności

Poprawka 138

Wniosek dotyczący dyrektywy
Załącznik II – punkt 5 c (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	5c. Internetowe punkty wymiany

UZASADNIENIE

1. Kontekst

Już w 2010 r. wezwano w ramach Europejskiej agendy cyfrowej do wprowadzenia instrumentów ustawodawczych służących realizacji polityki mającej na celu zapewnienie wysokiego poziomu bezpieczeństwa sieci i informacji. Ze względu na wzajemne powiązanie sieci i systemów informatycznych poważne zakłócenia sieci i systemów w jednym państwie członkowskim mogą mieć wpływ na inne państwa członkowskie i na Unię jako całość. Odporność i stabilność sieci i systemów informatycznych, a także ciągłość podstawowych usług mają zasadnicze znaczenie dla sprawnego funkcjonowania rynku wewnętrznego, zwłaszcza dla dalszego rozwoju jednolitego rynku cyfrowego.

Z uwagi na różne poziomy zdolności i rozdrobnienie podejścia w Unii Komisja Europejska dąży – za pomocą niniejszego wniosku dotyczącego dyrektywy w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii – do poprawy bezpieczeństwa internetu oraz prywatnych sieci i systemów informatycznych stanowiących podstawę funkcjonowania naszych społeczeństw i gospodarek.

W tym celu Komisja wymaga od państw członkowskich zwiększenia gotowości i ulepszenia wzajemnej współpracy. Natomiast operatorzy infrastruktury krytycznej w takich dziedzinach jak energetyka, transport i kluczowe usługi społeczeństwa informacyjnego, jak również organy administracji publicznej powinny podjąć odpowiednie działania mające na celu zarządzanie zagrożeniami bezpieczeństwa oraz zgłaszanie poważnych incydentów właściwym organom krajowym.

2. Projekt sprawozdania

Sprawozdawca popiera ogólny cel zaproponowanej dyrektywy, tj. zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji. Sprawozdawca uważa, że w celu zwiększenia skuteczności zaproponowanych środków niniejsza dyrektywa powinna w pierwszej kolejności ograniczać się do niektórych podmiotów, zapewniać ochronę poczynionych już inwestycji w bezpieczeństwo sieci i informacji oraz zapobiegać powielaniu struktur instytucjonalnych i obowiązków nakładanych na podmioty gospodarcze. Ponadto sprawozdawca jest zdania, że niniejsza dyrektywa powinna służyć rozwojowi opartych na zaufaniu relacji i wymianie informacji między sektorem publicznym a sektorem prywatnym oraz że należy unikać negatywnych reakcji w postaci zwykłej „kultury przestrzegania przepisów” zamiast pożądanej „kultury zarządzania zagrożeniami”. W obliczu powyższych rozwiązań sprawozdawca proponuje zwiększenie oddziaływania niniejszej dyrektywy poprzez wprowadzenie następujących istotnych zmian.

A. Zakres zastosowania

Projekt dyrektywy ma na celu nałożenie obowiązków na organy administracji publicznej i podmioty gospodarcze, m.in. w odniesieniu do infrastruktury krytycznej i usług społeczeństwa informacyjnego. Sprawozdawca uważa, że aby przepisy dyrektywy okazały się proporcjonalne i przyniosły szybkie rezultaty, obowiązkowe środki, o których mowa w rozdziale IV, powinny ograniczać się do infrastruktury krytycznej w węższym sensie. Jest on też zdania, że usług społeczeństwa informacyjnego nie należy zatem ujmować w załączniku II do niniejszej dyrektywy. Zamiast tego niniejsza dyrektywa powinna skupić się na podmiotach gospodarczych świadczących usługi m.in. w sektorze energetyki i transportu oraz usługi związane z opieką zdrowotną i infrastrukturą rynków finansowych.

Organy administracji publicznej – z uwagi na swoją misję publiczną – muszą zarządzać własnymi sieciami i systemami informatycznymi z należytą starannością. Dlatego sprawozdawca uważa za nieproporcjonalne nakładanie na nie takich samych obowiązków co na podmioty gospodarcze.
Poza zmianami dotyczącymi zakresu zastosowania sprawozdawca popiera niewyczerpujący charakter złącznika II i zgadza się na okresowy przegląd niniejszej dyrektywy, również w obliczu zmian technologicznych.

B. Właściwe organy krajowe

Wniosek dotyczący dyrektywy przewiduje wyznaczenie w każdym państwie członkowskim jednego właściwego organu krajowego odpowiedzialnego za monitorowanie wdrażania dyrektywy. Według sprawozdawcy nie uwzględnia to w dostatecznym stopniu istniejących już struktur.
W niektórych sektorach objętych zakresem niniejszej dyrektywy podmioty gospodarcze już teraz powiadamiają – formalnie lub nieformalnie – właściwy organ regulacyjny o pewnych incydentach związanych z bezpieczeństwem sieci i informacji. Z uwagi na bezpośrednie powiązanie i bliskie relacje ze swoim sektorem organy te posiadają dogłębną wiedzę o zagrożeniach i słabościach, zwłaszcza w odniesieniu do swojego sektora, i dlatego jak mało kto mogą ocenić konsekwencje ewentualnych lub aktualnych incydentów dla danego sektora.

Poza kwestią istniejących inwestycji sektorowych niektóre państwa członkowskie mogą być zmuszone – z powodu struktury konstytucyjnej lub z innych względów – wyznaczyć więcej niż jednen właściwy organ krajowy. Dlatego sprawozdawca proponuje zmianę dyrektywy umożliwiającą wyznaczenie przez każde państwo członkowskie więcej niż jednego właściwego organu. Jednak w celu zagwarantowania spójnego stosowania przepisów w danym państwie członkowskim oraz umożliwienia skutecznej i sprawnej współpracy na szczeblu Unii każde państwo członkowskie powinno powoływać jeden pojedynczy punkt kontaktowy odpowiedzialny m.in. za udział w sieci współpracy, o której mowa w art. 8, i za wydawanie wczesnych ostrzeżeń zgodnie z art. 10.

C. Sieć współpracy

Sprawozdawca uważa, że sieć współpracy – aby wzmocnić swoją działalność – powinna rozważyć zaproszenie w razie potrzeby do udziału podmiotów gospodarczych. Ponadto roczne sprawozdanie z działalności sieci dostarczyłoby cennych informacji na temat postępów w wymianie najlepszych praktyk przez państwa członkowskie i w rozwoju kwestii

zgłaszania incydentów w Unii.

D. Wymogi w zakresie bezpieczeństwa i zgłaszanie incydentów

Najważniejszą nowością jest wprowadzenie we wniosku dotyczącym dyrektywy obowiązku zgłaszania przez podmioty gospodarcze incydentów, które mają poważny wpływ na bezpieczeństwo podstawowych usług. W celu wyjaśnienia zakresu obowiązków i zakotwiczenia ich w akcie podstawowym sprawozdawca proponuje zastąpienie aktów delegowanych, o których mowa w art. 14 ust. 5, jasnymi kryteriami pozwalającymi określić znaczenie incydentów, które należy zgłaszać. Z uwagi na planowane ujednolicenie z dyrektywą 2009/140/WE wskaźniki podobne do wskaźników określonych w technicznych wytycznych ENISA dotyczących zgłaszania incydentów do celów dyrektywy 2009/140/WE pomogłyby wyjaśnić zakres i kryteria zgłoszenia. Ponadto sprawozdawca zaleca wzmocnienie zabezpieczeń dotyczących publikowania informacji na temat incydentów i wyjaśnia kwestię prawa właściwego, w przypadku gdy incydent ma wpływ na podstawowe usługi w kilku państwach członkowskich, aby nie nakładać licznych czy też niejasnych obowiązków dotyczących zgłaszania incydentów.

E. Wdrażanie i egzekwowanie

Sprawozdawca przypisuje zasadnicze znaczenie wzmocnieniu kultury zarządzania zagrożeniami i opieraniu się na dotychczasowych działaniach podmiotów gospodarczych. W tej kwestii jest on zdania, że najważniejsza jest ogólna współpraca i konkretne działania podejmowane przez podmioty gospodarcze, a nie sposób przekazywania informacji o konkretnych działaniach w zakresie zarządzania zagrożeniami.

Dlatego w kontekście art. 15 konieczna jest elastyczność dotycząca udowadniania spełnienia wymogów w zakresie bezpieczeństwa nałożonych na podmioty gospodarcze. Należy dopuścić inne formy udowadniania spełnienia wymogów niż audyt bezpieczeństwa.

F. Sankcje

Chociaż sprawozdawca dostrzega potrzebę przewidzenia sankcji wobec podmiotów gospodarczych niespełniających wymogów w celu zwiększenia skuteczności niniejszej dyrektywy, uważa, że ewentualne sankcje nie powinny zniechęcać do zgłaszania incydentów i powodować negatywnych skutków. Należy unikać sytuacji, w których ryzyko sankcji za m.in. zwykłe niespełnienie wymogów proceduralnych prowadziłoby do niezgłoszenia incydentu. Dlatego sprawozdawca sugeruje wyjaśnienie, że w przypadku kiedy podmiot gospodarczy nie wywiązał się z obowiązków przewidzianych w rozdziale IV, ale nie dopuścił się celowego lub rażącego zaniedbania, nie należy nakładać na niego sankcji.

19.12.2013

OPINIA KOMISJI PRZEMYSŁU, BADAŃ NAUKOWYCH I ENERGII*

dla Komisji Rynku Wewnętrznego i Ochrony Konsumentów

w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Sprawozdawczyni komisji opiniodawczej (*): Pilar del Castillo Vera

(*) Zaangażowana komisja – art. 50 Regulaminu

ZWIĘZŁE UZASADNIENIE

W lutym 2013 r., na wniosek Parlamentu Europejskiego zawarty w sprawozdaniu z własnej inicjatywy w sprawie Europejskiej agendy cyfrowej, Komisja Europejska przedstawiła wniosek dotyczący dyrektywy w sprawie środków mających na celu zapewnienie wysokiego poziomu bezpieczeństwa i informacji w całej Unii, wraz z pierwszą strategią bezpieczeństwa cybernetycznego UE. Sprawozdawczyni komisji opiniodawczej przyjmuje ten wniosek z zadowoleniem, mając na uwadze, że z analizy dostępnych danych wynika, iż incydenty o złośliwym charakterze związane z TIK mogą – dla samych tylko MŚP – pociągać za sobą szacunkowe koszty bezpośrednie rzędu ponad 560 mln euro rocznie, a wszystkie rodzaje incydentów (w tym problemy środowiskowe lub fizyczne, np. klęski żywiołowe) mogą powodować koszty rzędu ponad 2,3 mld.

Co do struktury wniosku, sprawozdawczyni zgadza się z szeregiem proponowanych środków, np. z rozszerzeniem przepisów dotyczących zgłaszania incydentów w zakresie bezpieczeństwa – obecnie ograniczonych do dostawców telekomunikacji zgodnie z art. 13a dyrektywy ramowej – na inne kluczowe sektory infrastruktury. W związku z tym takie propozycje jak wymóg, aby wszystkie państwa członkowskie posiadały odpowiednio funkcjonujące zespoły reagowania na incydenty komputerowe oraz wyznaczyły właściwy organ stanowiący element bezpiecznej ogólnoeuropejskiej sieci wymiany danych elektronicznych, umożliwiającej bezpieczne udostępnianie i wymianę informacji w zakresie bezpieczeństwa cybernetycznego, spotykają się z przychylnym przyjęciem i potencjalnie mogą wnieść znaczny wkład w cel proponowanej dyrektywy, którym jest zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii.

Sprawozdawczyni jest jednak zdania, że wniosek można udoskonalić, stosując doń dwie

główne zasady: efektywności i zaufania.

Zasad pierwsza – efektywność

Co do obowiązku państw członkowskich dotyczącego wyznaczenia właściwego organu odpowiedzialnego za monitorowanie stosowania dyrektywy we wszystkich sektorach wskazanych w załączniku II wniosku, sprawozdawczyni jest zdania, że każde państwo członkowskie nie tylko musi mieć swobodę wybrania takiego modelu zarządzania bezpieczeństwem cybernetycznym, jaki uważa za najbardziej odpowiedni, ale koniecznie trzeba uniknąć dublowania struktur instytucjonalnych, co mogłoby doprowadzić do konfliktów kompetencji oraz zakłóceń w komunikacji. W związku z tym sprawozdawczyni uważa, że nie należy przeszkadzać istniejącym strukturom krajowym, które skutecznie funkcjonują i reagują na potrzeby i wymogi konstytucyjne państw członkowskich. Sądzi jednak, że aby zagwarantować wymianę informacji na szczeblu Unii, wczesne powiadamianie o zagrożeniach i skuteczny udział w sieci współpracy, każde państwo członkowskie musi wyznaczyć **pojedynczy punkt kontaktowy**.

W tym samym duchu maksymalizowania efektywności proponowanej dyrektywy sprawozdawczyni jest zdania, że proponowane środki dotyczące ustanowienia krajowego **zespołu reagowania na incydenty komputerowe (CERT)** mogą okazać się niezupełnie odpowiednim wymogiem, ponieważ nie uwzględnia on różnych charakterów i składów istniejących zespołów. Większość państw członkowskich dysponuje więcej niż jednym CERT, a co więcej, zajmują się one różnymi rodzajami incydentów. Występują też różnice w liczbie i jakości działań zależnie od tego, czy są one organizowane i kierowane przez instytucje akademickie lub badawcze, rządy lub sektor prywatny. Dodatkowo wniosek w obecnej formie zakłóciłby funkcjonowanie istniejących międzynarodowych i europejskich sieci współpracy, do których zespoły CERT należą, a które okazały się skuteczne w koordynowaniu reakcji na incydenty na poziomie międzynarodowym i europejskim. W związku z powyższym sprawozdawczyni jest zdania, że zamiast odwoływania się do jednego krajowego CERT dyrektywa powinna być skierowana do tych CERT, które świadczą usługi na rzecz sektorów określonych w załączniku II, co oznaczałoby na przykład umożliwienie świadczenia przez jeden CERT usług na rzecz wszystkich sektorów wymienionych w załączniku II lub świadczenie przez kilka CERT usług na rzecz jednego i tego samego sektora. Sprawozdawczyni stoi jednak na stanowisku, że państwa członkowskie muszą zagwarantować pełną i nieprzerwaną w czasie operacyjność swoich CERT, a także zapewnić im wystarczające zasoby techniczne, finansowe i ludzkie, aby CERT należycie funkcjonowały oraz uczestniczyły w międzynarodowych i unijnych sieciach współpracy.

Zasada efektywności wymaga też wprowadzenia do proponowanej dyrektywy zmian dotyczących jej **zakresu**. Sprawozdawczyni zgadza się z tym, że rozszerzenie obowiązków w zakresie sprawozdawczości na sektor energii, transportu, zdrowia i finansów jest potrzebne, jednak propozycja objęcia środkami obowiązkowymi – określonymi w rozdziale IV – wszystkich działań rynkowych w „gospodarce internetowej" jest nieproporcjonalna i niewykonalna. Dlaczego nieproporcjonalna? Ponieważ bezkrytyczne nałożenie nowych obowiązków na otwartą i niezdefiniowaną kategorię, jaką jest każdy „dostawca usług społeczeństwa informacyjnego umożliwiających świadczenie innych usług społeczeństwa informacyjnego" jest nie tylko niezrozumiałe, ale też niewystarczająco uzasadnione w odniesieniu do ewentualnej szkody wyrządzonej przez incydent zagrażający

bezpieczeństwu oraz potencjalnie wiąże się z dodaniem kolejnej bariery biurokratycznej obciążającej nasz sektor przemysłu, a w szczególności MŚP. Dlaczego niewykonalna? Ponieważ istnieją poważne wątpliwości co do tego, czy właściwe organy będą w stanie poradzić sobie ze wszystkimi potencjalnymi zgłoszeniami w sposób proaktywny, który będzie zachęcał do dwukierunkowego dialogu z podmiotami gospodarczymi w celu rozwiązania kwestii zagrażających bezpieczeństwu.

W odniesieniu do **organów administracji publicznej** dyrektywa powinna zrównoważyć potrzebę dalszego rozwoju usług administracji elektronicznej z ustanowionymi już dla administracji publicznej obowiązkami należytej staranności w zakresie zarządzania swoimi sieciami i systemami informatycznymi oraz ich ochrony. W związku z tym sprawozdawczyni jest zdania, że chociaż wymogi wymiany informacji ustanowione w art. 14 powinny mieć w pełni zastosowanie do organów administracji publicznej, organy te nie powinny już podlegać obowiązkom określonym w art. 15.

Zasada druga – zaufanie

Sprawozdawczyni sądzi, że sukces tej dyrektywy zależy w znacznej mierze od umiejętnego aktywizowania uczestnictwa podmiotów gospodarczych, co doprowadziłoby do powstania wiarygodnego środowiska dla bezpieczeństwa sieci i informacji, w którym zaangażowane strony chciałyby proaktywnie uczestniczyć. Jeżeli dyrektywa tego nie osiągnie, będzie nieskuteczna. W związku z tym sprawozdawczyni proponuje zagwarantowanie podmiotom gospodarczym tego, że ich uczestnictwo i zgłoszenia nie będą miały takich negatywnych skutków, jak niepotrzebna publikacja incydentów w zakresie bezpieczeństwa, które podmioty te zgłosiły, lub pociągnięcie ich do odpowiedzialności przez właściwe organy lub pojedyncze punkty kontaktowe za utratę informacji. Konieczne jest też otwarcie dwukierunkowego dialogu między podmiotami a właściwymi organami, a uczestnictwo podmiotów gospodarczych musi być wspierane na wszystkich forach, w tym w ramach sieci współpracy.

Sprawozdawczyni jest też przekonana o tym, że zaufanie powinno być podstawą uczestnictwa właściwych organów lub pojedynczych punktów kontaktowych, zwłaszcza w odniesieniu do kwestii wymiany informacji. Aby to zapewnić, w omawianej dyrektywie powinny znaleźć swoje miejsce przepisy dotyczące poufności i wymogów bezpieczeństwa sieci.

POPRAWKI

Komisja Przemysłu, Badań Naukowych i Energii zwraca się do Komisji Rynku Wewnętrznego i Ochrony Konsumentów, jako do komisji przedmiotowo właściwej, o naniesienie w swoim sprawozdaniu następujących poprawek:

Poprawka 1

Wniosek dotyczący dyrektywy
Motyw 1

Tekst proponowany przez Komisję	*Poprawka*
(1) Sieci oraz systemy i usługi informatyczne pełnią w społeczeństwie istotną rolę. Ich niezawodność i bezpieczeństwo mają zasadnicze znaczenie dla działalności gospodarczej i dobrobytu społeczeństwa, a w szczególności dla funkcjonowania rynku wewnętrznego.	(1) Sieci oraz systemy i usługi informatyczne pełnią w społeczeństwie istotną rolę. Ich niezawodność i bezpieczeństwo mają zasadnicze znaczenie dla ***wolności i ogólnego bezpieczeństwa obywateli UE, a także dla*** działalności gospodarczej i dobrobytu społeczeństwa, a w szczególności dla funkcjonowania rynku wewnętrznego.

Poprawka 2

Wniosek dotyczący dyrektywy
Motyw 2

Tekst proponowany przez Komisję	*Poprawka*
(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.	(2) Skala***,*** częstotliwość ***i konsekwencje*** incydentów w obszarze bezpieczeństwa stają się coraz większe i stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. ***Systemy te mogą się również stać łatwym celem umyślnych szkodliwych działań, mających na celu uszkodzenie lub przerwanie działania tych systemów.*** Incydenty takie mogą ***zagrozić zdrowiu i bezpieczeństwu obywateli,*** utrudniać prowadzenie działalności gospodarczej, powodować znaczne straty finansowe, podważać zaufanie użytkowników ***i inwestorów*** oraz powodować znaczne straty w gospodarce Unii.

Uzasadnienie

Ataki cybernetyczne na spółki notowane na giełdzie są powszechne i obejmują kradzież aktywów finansowych, własności intelektualnej, a także przerwanie działalności ich klientów lub partnerów biznesowych i mogą mieć wpływ na stosunki z akcjonariuszami, a także decyzje potencjalnych inwestorów.

Poprawka 3

Wniosek dotyczący dyrektywy
Motyw 3

Tekst proponowany przez Komisję	*Poprawka*
(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.	(3) Jako narzędzia komunikacji ***funkcjonujące ponad tradycyjnymi granicami,*** cyfrowe systemy informatyczne, a przede wszystkim internet, odgrywają istotną rolę w ułatwianiu transgranicznego przepływu towarów, usług***, idei*** 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***, a także dla funkcjonowania rynków zewnętrznych***.

Uzasadnienie

Odporność i stabilność sieci i systemów informatycznych rynku wewnętrznego ma także zasadnicze znaczenie dla interakcji z rynkami globalnymi i regionalnymi, takimi jak Ameryka Północna, Azja itd.

Poprawka 4

Wniosek dotyczący dyrektywy
Motyw 4

Tekst proponowany przez Komisję	*Poprawka*
(4) Na poziomie Unii należy ustanowić mechanizm współpracy, który umożliwi wymianę informacji i podejmowanie skoordynowanych działań w zakresie wykrywania i reagowania w odniesieniu do bezpieczeństwa sieci i informacji. Aby mechanizm ten był skuteczny i dostępny dla wszystkich, konieczne jest, by	(4) Na poziomie Unii należy ustanowić mechanizm współpracy, który umożliwi wymianę informacji i podejmowanie skoordynowanych działań w zakresie ***zapobiegania,*** wykrywania i reagowania w odniesieniu do bezpieczeństwa sieci i informacji. Aby mechanizm ten był skuteczny i dostępny dla wszystkich,

wszystkie państwa członkowskie posiadały minimalne zdolności i strategię zapewniające wysoki poziom bezpieczeństwa sieci i informacji na ich terytorium. Aby promować kulturę wspierającą przeciwdziałanie zagrożeniom i zapewnić zgłaszanie najpoważniejszych incydentów, należy wprowadzić minimalne wymogi w zakresie bezpieczeństwa również w odniesieniu do ***organów administracji publicznej*** i operatorów ***krytycznej*** infrastruktury teleinformatycznej.	konieczne jest, by wszystkie państwa członkowskie posiadały minimalne zdolności i strategię zapewniające wysoki poziom bezpieczeństwa sieci i informacji na ich terytorium. Aby promować kulturę wspierającą przeciwdziałanie zagrożeniom i zapewnić zgłaszanie najpoważniejszych incydentów, należy wprowadzić minimalne wymogi w zakresie bezpieczeństwa również w odniesieniu do ***publicznych*** i ***prywatnych*** operatorów infrastruktury teleinformatycznej***, a także spółek notowanych na giełdzie***. ***Ramy prawne powinny opierać się na potrzebie zabezpieczenia prywatności i integralności obywateli. Sieci ostrzegania o zagrożeniach infrastruktury strategicznej należy rozszerzyć na tych konkretnych operatorów.***

Uzasadnienie

Incydenty dotyczące bezpieczeństwa w spółkach notowanych na giełdzie mogą znacznie wpłynąć na produkty firmy, usługi, stosunki z klientami lub dostawcami, a także ogólnie na warunki konkurencji, a tym samym mogą mieć duży wpływ na funkcjonowanie rynku wewnętrznego (i zewnętrznego). Dlatego niniejszą dyrektywą należy objąć także spółki notowane na giełdzie.

Poprawka 5

Wniosek dotyczący dyrektywy
Motyw 4 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(4a) Niniejsza dyrektywa powinna skupiać się na infrastrukturze krytycznej, która ma zasadnicze znaczenie dla utrzymania kluczowych działań gospodarczych i społecznych w dziedzinach energetyki, transportu, bankowości, infrastruktur rynków finansowych oraz opieki zdrowotnej.

Poprawka 6

Wniosek dotyczący dyrektywy
Motyw 4 b (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(4b) Aby nie dopuścić do przekraczania lub nadużywania uprawnień przez rządy, konieczne jest, by systemy informatyczne i bezpieczeństwa w urzędach publicznych były przejrzyste, uzasadnione, dobrze zdefiniowane i przyjęte w przejrzysty sposób w procesie demokratycznym.

Poprawka 7

Wniosek dotyczący dyrektywy
Motyw 6

Tekst proponowany przez Komisję	*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.	(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 podmiotów gospodarczych uniemożliwia z kolei ustanowienie globalnego i skutecznego mechanizmu współpracy na poziomie Unii***, szkodząc dodatkowo skuteczności współpracy międzynarodowej, a w konsekwencji – walce z globalnymi wyzwaniami w dziedzinie bezpieczeństwa, oraz podważa wiodącą pozycję Unii na szczeblu międzynarodowym w zabezpieczaniu i propagowaniu wolnego, wydajnego i bezpiecznego internetu***.

Poprawka 8

Wniosek dotyczący dyrektywy
Motyw 7

Tekst proponowany przez Komisję	*Poprawka*
(7) Skuteczne reagowanie na wyzwania związane z zapewnieniem bezpieczeństwa sieci i systemów informatycznych wymaga zatem przyjęcia całościowego podejścia na poziomie Unii, które będzie obejmować wprowadzenie wymogów dotyczących budowania i planowania wspólnych minimalnych zdolności, wymianę informacji i koordynację działań oraz wprowadzenie wspólnych minimalnych wymogów w zakresie bezpieczeństwa ***dla wszystkich podmiotów gospodarczych, których dotyczy ten problem, oraz dla organów administracji publicznej***.	(7) Skuteczne reagowanie na wyzwania związane z zapewnieniem bezpieczeństwa sieci i systemów informatycznych wymaga zatem przyjęcia całościowego podejścia na poziomie Unii, które będzie obejmować wprowadzenie wymogów dotyczących budowania i planowania wspólnych minimalnych zdolności, ***rozwijanie umiejętności z zakresu bezpieczeństwa cybernetycznego,*** wymianę informacji i koordynację działań oraz wprowadzenie wspólnych minimalnych wymogów w zakresie bezpieczeństwa. ***Minimalne wspólne normy należy stosować zgodnie z odpowiednimi zaleceniami grup koordynacji bezpieczeństwa cybernetycznego.***

Poprawka 9

Wniosek dotyczący dyrektywy
Motyw 9

Tekst proponowany przez Komisję	*Poprawka*
(9) W celu osiągnięcia i utrzymania wspólnego wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych każde państwo członkowskie powinno posiadać krajową strategię w zakresie bezpieczeństwa sieci i informacji określającą cele strategiczne i konkretne działania, które należy wdrożyć. Na ***poziome*** krajowym należy opracować spełniające zasadnicze wymagania plany współpracy w zakresie bezpieczeństwa	(9) W celu osiągnięcia i utrzymania wspólnego wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych każde państwo członkowskie powinno posiadać krajową strategię w zakresie bezpieczeństwa sieci i informacji określającą cele strategiczne i konkretne działania, które należy wdrożyć. ***W oparciu o minimalne wymogi ustanowione w niniejszej dyrektywie*** na ***poziomie*** krajowym należy opracować

sieci i informacji, tak aby osiągnąć poziom zdolności reagowania umożliwiający skuteczną i sprawną współpracę na poziomach krajowym i unijnym w przypadku wystąpienia incydentów.	spełniające zasadnicze wymagania plany współpracy w zakresie bezpieczeństwa sieci i informacji, tak aby osiągnąć poziom zdolności reagowania umożliwiający skuteczną i sprawną współpracę na poziomach krajowym i unijnym w przypadku wystąpienia incydentów. ***Każde państwo członkowskie powinno zatem być zobowiązane do wypełniania wspólnych norm dotyczących formatu i wymienialności danych, które mają być udostępniane i oceniane. Państwa członkowskie mogą zwrócić się do Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) o pomoc w opracowywaniu krajowych strategii w zakresie bezpieczeństwa sieci i informacji na podstawie wspólnej minimalnej strategii w zakresie bezpieczeństwa sieci i informacji.***

Uzasadnienie

ENISA jest już uznawana przez odpowiednie zainteresowane strony za wysoce kompetentny ośrodek doskonałości i godne zaufania narzędzie promowania bezpieczeństwa cybernetycznego w UE. Dlatego UE powinna unikać powielania wysiłków i struktur poprzez oparcie się na know-how ENISA i powinna wymagać od ENISA oferowania usług doradczych tym państwom członkowskim, którym brakuje instytucji z zakresu bezpieczeństwa sieci i informacji oraz specjalistycznej wiedzy i które zwracają się o takie wsparcie.

Poprawka 10

Wniosek dotyczący dyrektywy
Motyw 10

Tekst proponowany przez Komisję	*Poprawka*
(10) W celu umożliwienia skutecznego wprowadzenia w życie przepisów przyjętych zgodnie z niniejszą dyrektywą w każdym państwie członkowskim należy ustanowić lub wyznaczyć organ odpowiedzialny za koordynowanie kwestii związanych z bezpieczeństwem sieci i informacji oraz działający jako centralny punkt kontaktowy ds. współpracy	(10) W celu umożliwienia skutecznego wprowadzenia w życie przepisów przyjętych zgodnie z niniejszą dyrektywą w każdym państwie członkowskim należy ustanowić lub wyznaczyć organ odpowiedzialny za koordynowanie kwestii związanych z bezpieczeństwem sieci i informacji oraz działający jako ***pojedynczy*** centralny punkt kontaktowy ds.

transgranicznej na poziomie UE. Organom tym należy zapewnić wystarczające zasoby techniczne, finansowe i ludzkie, aby mogły one skutecznie i efektywnie realizować powierzone im zadania w celu osiągnięcia celów niniejszej dyrektywy.

koordynacji wewnętrznej i współpracy transgranicznej na poziomie UE. ***Pojedyncze krajowe punkty kontaktowe powinny być wyznaczane bez uszczerbku dla możliwości wyznaczenia przez państwo członkowskie więcej niż jednego właściwego organu odpowiedzialnego za bezpieczeństwo sieci i informacji zgodnie z ich wymogami konstytucjonalnymi, jurysdykcyjnymi lub administracyjnymi, ale muszą one posiadać mandat do koordynacji na szczeblu krajowym i unijnym.*** Organom tym należy zapewnić wystarczające zasoby techniczne, finansowe i ludzkie, aby mogły one ***stale,*** skutecznie i efektywnie realizować powierzone im zadania w celu osiągnięcia celów niniejszej dyrektywy.

Poprawka 11

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 już istniejących ustaleń sektorowych i unikania powielania należy umożliwić państwom członkowskim wyznaczanie więcej niż jednego właściwego organu 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 wyznaczyło tylko jeden krajowy pojedynczy punkt kontaktowy odpowiedzialny za współpracę transgraniczną na szczeblu Unii. Jeżeli wymagają tego struktury konstytucyjne lub inne ustalenia danego państwa członkowskiego, powinno mieć ono

możliwość wyznaczenia tylko jednego organu, który będzie wykonywał zadania właściwego organu i pojedynczego punktu kontaktowego.

Poprawka 12

Wniosek dotyczący dyrektywy
Motyw 11

Tekst proponowany przez Komisję	*Poprawka*
(11) Wszystkie państwa członkowskie powinny zostać odpowiednio wyposażone, zarówno pod względem zdolności technicznych, jak i możliwości organizacyjnych, w celu zapobiegania incydentom i zagrożeniom dotyczącym sieci i systemów informatycznych, wykrywania ich, reagowania na nie i łagodzenia ich skutków. We wszystkich państwach członkowskich należy zatem ustanowić sprawnie funkcjonujące i spełniające zasadnicze wymagania zespoły reagowania na incydenty komputerowe, które zagwarantują skuteczne i kompatybilne zdolności reagowania na incydenty i zagrożenia oraz zapewnią skuteczną współpracę na poziomie unijnym.	(11) Wszystkie państwa członkowskie ***i podmioty gospodarcze*** powinny zostać odpowiednio wyposażone, zarówno pod względem zdolności technicznych, jak i możliwości organizacyjnych, w celu zapobiegania incydentom i zagrożeniom dotyczącym sieci i systemów informatycznych, wykrywania ich, reagowania na nie i łagodzenia ich skutków ***w dowolnym momencie***. ***Systemy bezpieczeństwa administracji publicznej muszą być bezpieczne i podlegać demokratycznej kontroli i nadzorowi. Wspólnie wymagane wyposażenie i zdolności muszą odpowiadać wspólnie uzgodnionym normom technicznym oraz standardowym procedurom działania.*** We wszystkich państwach członkowskich należy zatem ustanowić sprawnie funkcjonujące i spełniające zasadnicze wymagania zespoły reagowania na incydenty komputerowe ***(CERT)***, które zagwarantują skuteczne i kompatybilne zdolności reagowania na incydenty i zagrożenia oraz zapewnią skuteczną współpracę na poziomie unijnym. ***CERT powinny mieć możliwość interakcji na podstawie wspólnych standardów technicznych i standardowych procedur działania. Z uwagi na różne cechy istniejących CERT, które odpowiadają różnym potrzebom tematycznym i podmiotom, państwa członkowskie powinny zagwarantować, że każdy sektor***

objęty załącznikiem II jest obsługiwany przez co najmniej jeden CERT. W odniesieniu do współpracy transgranicznej CERT państwa członkowskie powinny dołożyć starań, aby CERT posiadały środki wystarczające do udziału w już działających międzynarodowych i europejskich sieciach współpracy.

Uzasadnienie

Należy zapewnić interoperacyjność.

Poprawka 13

Wniosek dotyczący dyrektywy
Motyw 12

Tekst proponowany przez Komisję	*Poprawka*
(12) Opierając się na znacznych postępach dokonanych w ramach europejskiego forum państw członkowskich (EFMS), które umożliwiły prowadzenie dialogu i wymianę doświadczeń dotyczących sprawdzonych rozwiązań, w tym opracowywanie zasad współpracy na wypadek kryzysów cybernetycznych w Europie, państwa członkowskie i Komisja powinny stworzyć sieć w celu zapewnienia ich stałej komunikacji i wsparcia ich współpracy. Ten bezpieczny i skuteczny mechanizm współpracy powinien umożliwić uporządkowaną i skoordynowaną wymianę informacji, wykrywanie incydentów oraz reagowanie na nie na poziomie Unii.	(12) Opierając się na znacznych postępach dokonanych w ramach europejskiego forum państw członkowskich (EFMS), które umożliwiły prowadzenie dialogu i wymianę doświadczeń dotyczących sprawdzonych rozwiązań, w tym opracowywanie zasad współpracy na wypadek kryzysów cybernetycznych w Europie, państwa członkowskie i Komisja powinny stworzyć sieć w celu zapewnienia ich stałej komunikacji i wsparcia ich współpracy. Ten bezpieczny i skuteczny mechanizm współpracy***, w którym zapewnia się udział podmiotów gospodarczych,*** powinien umożliwić uporządkowaną i skoordynowaną wymianę informacji, wykrywanie incydentów oraz reagowanie na nie na poziomie Unii.

Poprawka 14

Wniosek dotyczący dyrektywy
Motyw 13

Tekst proponowany przez Komisję	*Poprawka*
(13) Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA) powinna wspierać działania państw członkowskich i Komisji poprzez zapewnianie wiedzy specjalistycznej i doradztwa oraz poprzez ułatwianie wymiany najlepszych praktyk. W szczególności ***Komisja powinna*** konsultować się z ENISA przy stosowaniu niniejszej dyrektywy. W celu zapewnienia skutecznego i terminowego informowania państw członkowskich i Komisji wczesne ostrzeżenia dotyczące incydentów i zagrożeń należy zgłaszać poprzez sieć współpracy. Aby budować zdolności i wiedzę wśród państw członkowskich, sieć współpracy powinna również służyć jako narzędzie wymiany najlepszych praktyk, pomagać członkom w budowaniu zdolności oraz kierować organizacją wzajemnej weryfikacji i ćwiczeń w zakresie bezpieczeństwa sieci i informacji.	(13) Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA) powinna wspierać działania państw członkowskich i Komisji poprzez zapewnianie wiedzy specjalistycznej i doradztwa oraz poprzez ułatwianie wymiany najlepszych praktyk. ***Komisja i państwa członkowskie powinny*** w szczególności konsultować się z ENISA przy stosowaniu niniejszej dyrektywy. W celu zapewnienia skutecznego i terminowego informowania państw członkowskich i Komisji wczesne ostrzeżenia dotyczące incydentów i zagrożeń należy zgłaszać poprzez sieć współpracy. Aby budować zdolności i wiedzę wśród państw członkowskich, sieć współpracy powinna również służyć jako narzędzie wymiany najlepszych praktyk, pomagać członkom w budowaniu zdolności oraz kierować organizacją wzajemnej weryfikacji i ćwiczeń w zakresie bezpieczeństwa sieci i informacji.

Poprawka 15

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 ***pod nadzorem ENISA***. 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

techniczne i finansowe oraz zasoby ludzkie, jak również ich infrastruktura łączności, gwarantują ich skuteczne, sprawne i bezpieczne uczestnictwo w sieci.	zasoby i procedury techniczne i finansowe oraz zasoby ludzkie, jak również ich infrastruktura łączności, gwarantują ich skuteczne, sprawne i bezpieczne uczestnictwo w sieci. ***Aby sieć współpracy była w stanie skutecznie realizować swoją misję, Komisja powinna ustanowić dla niej pozycję w budżecie.***

Poprawka 16

Wniosek dotyczący dyrektywy
Motyw 14 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(14a) W stosownych przypadkach do udziału w działaniach sieci współpracy można również zaprosić podmioty gospodarcze.

Poprawka 17

Wniosek dotyczący dyrektywy
Motyw 15

Tekst proponowany przez Komisję	*Poprawka*
(15) Ponieważ większość sieci i systemów informatycznych eksploatowana jest przez podmioty prywatne, niezbędna jest współpraca między sektorem publicznym i prywatnym. Podmioty gospodarcze należy zachęcać do tworzenia własnych nieformalnych mechanizmów współpracy w celu zapewnienia bezpieczeństwa sieci i informacji. Powinny one również współpracować z sektorem publicznym oraz dzielić się ***z nim*** informacjami i najlepszymi praktykami ***w zamian za*** wsparcie operacyjne w przypadku incydentów.	(15) Ponieważ większość sieci i systemów informatycznych eksploatowana jest przez podmioty prywatne, niezbędna jest współpraca między sektorem publicznym i prywatnym. Podmioty gospodarcze należy zachęcać do tworzenia własnych nieformalnych mechanizmów współpracy w celu zapewnienia bezpieczeństwa sieci i informacji. Powinny one również współpracować z sektorem publicznym oraz dzielić się ***obustronnie*** informacjami i najlepszymi praktykami***, co obejmuje także wzajemną wymianę odpowiednich informacji,*** wsparcie operacyjne ***i informacje analizowane pod kątem strategicznym*** w przypadku incydentów. ***W celu aktywnego zachęcania do dzielenia***

	się informacjami oraz najlepszymi praktykami konieczne jest zapewnienie, by podmioty gospodarcze uczestniczące w wymianie nie doświadczały strat w wyniku tej współpracy. Konieczne są odpowiednie zabezpieczenia w celu zapewnienia, by tego rodzaju współpraca nie narażała takich podmiotów na wyższe ryzyko braku zgodności lub na nowe zobowiązania na podstawie m.in. prawa konkurencji, własności intelektualnej, ochrony danych czy cyberprzestępczości oraz by nie narażała ich na podwyższone ryzyko operacyjne lub związane z bezpieczeństwem.

Poprawka 18

Wniosek dotyczący dyrektywy
Motyw 16

Tekst proponowany przez Komisję	*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***.	(16) W celu zapewnienia przejrzystości i w celu odpowiedniego informowania obywateli UE i podmiotów gospodarczych ***pojedyncze punkty kontaktowe*** powinny założyć wspólną ***ogólnounijną*** stronę internetową, na której publikowane będą niemające poufnego charakteru informacje na temat incydentów***, zagrożeń*** i ***sposobów ich łagodzenia oraz gdzie w ostateczności będzie się udzielać porad dotyczących odpowiedniej obsługi technicznej***.

Poprawka 19

Wniosek dotyczący dyrektywy
Motyw 17

Tekst proponowany przez Komisję	*Poprawka*
(17) W przypadku gdy informacje uznaje	(17) ***Polityka klasyfikacji informacji, o***

się za poufne zgodnie z unijnymi i krajowymi przepisami dotyczącymi tajemnicy handlowej, w trakcie wykonywania czynności i realizacji celów określonych w niniejszej dyrektywie należy zapewnić taką poufność.	***której mowa w motywie 14, powinna być zgodna z zalecanym przez ENISA protokołem TLP. Wszelkie wymieniane informacje mają być klasyfikowane i przetwarzane według ich stopnia wrażliwości określonego przez źródło informacji.*** W przypadku gdy informacje uznaje się za poufne zgodnie z unijnymi i krajowymi przepisami dotyczącymi tajemnicy handlowej, w trakcie wykonywania czynności i realizacji celów określonych w niniejszej dyrektywie należy zapewnić taką poufność.

Poprawka 20

Wniosek dotyczący dyrektywy
Motyw 18

Tekst proponowany przez Komisję	*Poprawka*
(18) Na podstawie zwłaszcza krajowych doświadczeń w zarządzaniu kryzysowym i we współpracy z ENISA Komisja i państwa członkowskie powinny opracować unijny plan współpracy w zakresie bezpieczeństwa sieci i informacji określający mechanizmy współpracy służące ***do zwalczania zagrożeń i incydentów***. Plan ten należy odpowiednio uwzględniać podczas korzystania z systemu wczesnego ostrzegania w ramach sieci współpracy.	(18) Na podstawie zwłaszcza krajowych doświadczeń w zarządzaniu kryzysowym i we współpracy z ENISA Komisja i państwa członkowskie powinny opracować unijny plan współpracy w zakresie bezpieczeństwa sieci i informacji określający mechanizmy współpracy ***oraz najlepsze praktyki i wzorce działania*** służące ***zapobieganiu zagrożeniom i incydentom oraz ich wykrywaniu, zgłaszaniu i zwalczaniu***. Plan ten należy odpowiednio uwzględniać podczas korzystania z systemu wczesnego ostrzegania w ramach sieci współpracy.

Poprawka 21

Wniosek dotyczący dyrektywy
Motyw 19

Tekst proponowany przez Komisję	*Poprawka*
(19) Przekazywanie wczesnych ostrzeżeń w ramach sieci powinno być wymagane	(19) Przekazywanie wczesnych ostrzeżeń w ramach sieci powinno być wymagane

tylko w przypadku, gdy skala i waga danego incydentu lub zagrożenia są lub mogą być w przyszłości na tyle znaczące, że konieczna jest wymiana informacji lub koordynacja reakcji na poziomie Unii. Wczesne ostrzeżenia powinny być zatem ograniczone do ***rzeczywistych lub potencjalnych*** incydentów lub zagrożeń, które się szybko rozwijają, przekraczają krajowe zdolności reagowania lub mają wpływ na więcej niż jedno państwo członkowskie. W celu umożliwienia właściwej oceny wszystkie informacje niezbędne do oceny zagrożenia lub incydentu należy przekazywać do sieci współpracy.	tylko w przypadku, gdy skala i waga danego incydentu lub zagrożenia są lub mogą być w przyszłości na tyle znaczące, że konieczna jest wymiana informacji lub koordynacja reakcji na poziomie Unii. Wczesne ostrzeżenia powinny być zatem ograniczone do incydentów lub zagrożeń, które się szybko rozwijają, przekraczają krajowe zdolności reagowania lub mają wpływ na więcej niż jedno państwo członkowskie. W celu umożliwienia właściwej oceny wszystkie informacje niezbędne do oceny zagrożenia lub incydentu należy przekazywać do sieci współpracy.

Poprawka 22

Wniosek dotyczący dyrektywy
Motyw 20

Tekst proponowany przez Komisję	*Poprawka*
(20) Po otrzymaniu wczesnego ostrzeżenia i dokonaniu jego oceny ***właściwe organy*** powinny uzgodnić skoordynowaną reakcję zgodnie z unijnym planem współpracy w zakresie bezpieczeństwa sieci i informacji. O środkach przyjętych na poziomie krajowym w wyniku skoordynowanej reakcji należy poinformować ***właściwe organy*** oraz Komisję.	(20) Po otrzymaniu wczesnego ostrzeżenia i dokonaniu jego oceny ***pojedyncze punkty kontaktowe*** powinny uzgodnić skoordynowaną reakcję zgodnie z unijnym planem współpracy w zakresie bezpieczeństwa sieci i informacji. O środkach przyjętych na poziomie krajowym w wyniku skoordynowanej reakcji należy poinformować ***pojedyncze punkty kontaktowe, ENISA*** oraz Komisję.

Poprawka 23

Wniosek dotyczący dyrektywy
Motyw 22

Tekst proponowany przez Komisję	*Poprawka*
(22) Odpowiedzialność za zapewnienie	(22) Odpowiedzialność za zapewnienie

bezpieczeństwa sieci i informacji w dużym stopniu spoczywa na organach administracji publicznej i podmiotach gospodarczych. Za pomocą stosownych wymogów regulacyjnych i dobrowolnych praktyk branżowych należy wspierać i rozwijać kulturę przeciwdziałania zagrożeniom, obejmującą przeprowadzanie ocen zagrożenia i wdrażanie środków bezpieczeństwa stosownych do danego zagrożenia. Stworzenie równych warunków działania ma również kluczowe znaczenie dla skutecznego funkcjonowania sieci współpracy w celu zapewnienia skutecznej współpracy ze strony wszystkich państw członkowskich.

bezpieczeństwa sieci i informacji w dużym stopniu spoczywa na organach administracji publicznej i podmiotach gospodarczych. Za pomocą stosownych wymogów regulacyjnych i dobrowolnych praktyk branżowych należy wspierać i rozwijać kulturę przeciwdziałania zagrożeniom, ***ścisłej współpracy i zaufania,*** obejmującą przeprowadzanie ocen zagrożenia i wdrażanie środków bezpieczeństwa stosownych do danego zagrożenia. Stworzenie ***godnych zaufania,*** równych warunków działania ma również kluczowe znaczenie dla skutecznego funkcjonowania sieci współpracy w celu zapewnienia skutecznej współpracy ze strony wszystkich państw członkowskich.

Poprawka 24

Wniosek dotyczący dyrektywy
Motyw 24

Tekst proponowany przez Komisję	*Poprawka*
(24) Obowiązki te powinny obejmować nie tylko sektor łączności elektronicznej, lecz również głównych dostawców usług społeczeństwa informacyjnego, określonych w dyrektywie 98/34/WE Parlamentu Europejskiego i Rady z dnia 22 czerwca 1998 r. ustanawiającej procedurę udzielania informacji w dziedzinie norm i przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego[27], na których opierają się pochodne usługi społeczeństwa informacyjnego oraz działania ***w*** prowadzone w internecie, takie jak platformy handlu elektronicznego, internetowe portale płatnicze, portale społecznościowe, wyszukiwarki, usługi chmur obliczeniowych***,*** sklepy z aplikacjami***. Zakłócenia tych podstawowych usług społeczeństwa informacyjnego uniemożliwiają świadczenie innych usług społeczeństwa***	(24) Obowiązki te powinny obejmować nie tylko sektor łączności elektronicznej, lecz również ***operatorów infrastruktury, którzy są w dużym stopniu uzależnieni od technologii informacyjnych i komunikacyjnych i którzy mają kluczowe znaczenie dla utrzymania istotnych funkcji gospodarczych lub społecznych, takich jak dostawy energii elektrycznej i gazu, usługi transportowe, działalność instytucji kredytowych, infrastruktura rynków finansowych i opieka zdrowotna. Zakłócenia tych sieci i systemów informatycznych miałyby wpływ na rynek wewnętrzny. O ile obowiązki określone w niniejszej dyrektywie nie obejmują*** głównych dostawców usług społeczeństwa informacyjnego, określonych w dyrektywie 98/34/WE Parlamentu Europejskiego i Rady z dnia 22 czerwca 1998 r. ustanawiającej procedurę udzielania informacji w dziedzinie norm i przepisów

informacyjnego**, **dla których stanowią one podstawę. Twórcy oprogramowania i producenci sprzętu nie są dostawcami usług społeczeństwa informacyjnego, a zatem nie są oni objęci zakresem powyższych przepisów. Obowiązki te powinny również zostać rozszerzone na organy administracji publicznej oraz operatorów infrastruktury krytycznej, którzy są w dużym stopniu uzależnieni od technologii informacyjnych i komunikacyjnych i którzy mają kluczowe znaczenie dla utrzymania istotnych funkcji gospodarczych i społecznych, takich jak dostawy energii elektrycznej i gazu, usługi transportowe oraz działalność instytucji kredytowych, giełd papierów wartościowych i placówek opieki zdrowotnej. Zakłócenia tych sieci i systemów informatycznych miałyby wpływ na rynek wewnętrzny.

technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego[27], na których opierają się pochodne usługi społeczeństwa informacyjnego oraz działania prowadzone w internecie, takie jak platformy handlu elektronicznego, internetowe portale płatnicze, portale społecznościowe, wyszukiwarki, usługi chmur obliczeniowych ***ogólnie lub*** sklepy z aplikacjami***, mogą one na zasadzie dobrowolności informować właściwy organ lub pojedynczy punkt kontaktowy o tych incydentach związanych z bezpieczeństwem sieci**, **które uznają za stosowne, a właściwy organ lub pojedynczy punkt kontaktowy powinien, na ile to możliwe, przedstawić podmiotom gospodarczym, które powiadomiły o incydencie, informacje analizowane pod kątem strategicznym, które pomogą przezwyciężyć zagrożenie dla bezpieczeństwa.***

---

[27] Dz.U. L 204 z 21.7.1998, s. 37.

[27] Dz.U. L 204 z 21.7.1998, s. 37.

Poprawka 25

Wniosek dotyczący dyrektywy
Motyw 25

Tekst proponowany przez Komisję	*Poprawka*
(25) Nałożenie na ***organy administracji publicznej i*** podmioty gospodarcze obowiązku wprowadzenia środków organizacyjnych i technicznych nie powinno wiązać się z koniecznością zaprojektowania, opracowania i wyprodukowania specjalnego komercyjnego produktu informatycznego w określony sposób.	(25) Nałożenie na podmioty gospodarcze obowiązku wprowadzenia środków organizacyjnych i technicznych nie powinno wiązać się z koniecznością zaprojektowania, opracowania i wyprodukowania specjalnego komercyjnego produktu informatycznego w określony sposób. ***Z drugiej strony należy wymagać stosowania międzynarodowych norm dotyczących bezpieczeństwa cybernetycznego.***

Poprawka 26

Wniosek dotyczący dyrektywy
Motyw 28

Tekst proponowany przez Komisję	*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.	(28) Właściwe organy ***i pojedyncze punkty kontaktowe*** powinny zwracać należytą uwagę na zachowanie nieformalnych i bezpiecznych kanałów wymiany informacji między podmiotami gospodarczymi i między sektorami publicznym i prywatnym. ***Informacje o nieznanych wcześniej słabych punktach i incydentach zgłoszonych odpowiednim organom powinny zostać przekazane producentom i dostawcom usług danych usług i produktów TIK.*** Decyzje o informowaniu społeczeństwa o incydentach zgłoszonych właściwym organom ***i pojedynczym punktom kontaktowym*** 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 podmioty gospodarcze zgłaszające incydenty. ***Aby zagwarantować zaufanie i skuteczność, informowanie społeczeństwa o incydentach następuje wyłącznie po konsultacji z podmiotami, które zgłosiły incydent, i tylko wówczas, gdy jest to absolutnie niezbędne do osiągnięcia celów niniejszej dyrektywy.*** Wykonując obowiązki w zakresie powiadamiania, właściwe organy ***i pojedyncze punkty kontaktowe*** powinny zwracać szczególną uwagę na potrzebę zachowania poufności w odniesieniu do informacji dotyczących słabych punktów produktów, aż do momentu ***zastosowania*** stosownych rozwiązań problemów bezpieczeństwa***, ale nie opóźniać bardziej niż jest to wymagane żadnego powiadomienia***. ***Z***

	zasady pojedyncze punkty kontaktowe nie powinny ujawniać danych osobowych osób zaangażowanych w incydenty. Pojedyncze punkty kontaktowe powinny ujawniać dane osobowe wyłącznie wtedy, kiedy ujawnienie takich danych jest niezbędne i współmierne do celu, w którym są ujawniane.

Uzasadnienie

W przypadku gdy organy są świadome słabych punktów pewnych produktów i usług TIK, powinny one powiadomić producentów i dostawców usług, tak by mogli oni w odpowiednim czasie dostosować swoje produkty i usługi.

Poprawka 27

Wniosek dotyczący dyrektywy
Motyw 29

Tekst proponowany przez Komisję	*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.	(29) Właściwe organy ***i pojedyncze punkty kontaktowe*** powinny dysponować niezbędnymi środkami do wykonywania swoich obowiązków, w tym uprawnieniami do uzyskiwania wystarczających informacji od podmiotów gospodarczych, w celu oceny poziomu bezpieczeństwa sieci i systemów informatycznych, ***zmierzenia liczby, skali i zakresu incydentów,*** jak również wiarygodnymi i pełnymi danymi na temat incydentów, które mają wpływ na funkcjonowanie sieci i systemów informatycznych.

Poprawka 28

Wniosek dotyczący dyrektywy
Motyw 30

Tekst proponowany przez Komisję	*Poprawka*
(30) Źródłem incydentu w wielu	(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, 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.

przypadkach jest działalność przestępcza ***lub wojna cybernetyczna***. Przestępczy charakter incydentów można podejrzewać nawet wtedy, gdy początkowo dowody nie są wystarczająco przekonujące. W tym kontekście odpowiednia współpraca między właściwymi organami ***lub pojedynczymi punktami kontaktowymi a*** organami ścigania ***oraz z EC3 (ośrodek Europolu ds. cyberprzestępczości) i z ENISA*** powinna stanowić część skutecznej i kompleksowej reakcji na zagrożenie związane z możliwością wystąpienia incydentu zagrażającego 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.

Poprawka 29

Wniosek dotyczący dyrektywy
Motyw 31

Tekst proponowany przez Komisję	*Poprawka*
(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	(31) W wyniku incydentów w wielu przypadkach istnieje niebezpieczeństwo naruszenia danych osobowych. ***Państwa członkowskie i podmioty gospodarcze powinny chronić przechowywane, przetwarzane lub przekazywane dane osobowe przed przypadkowym lub nielegalnym zniszczeniem, przypadkową utratą lub zmianą, a także niedozwolonym lub nielegalnym przechowywaniem, dostępem lub ujawnieniem, rozpowszechnianiem lub dostępem, i zapewnić wprowadzanie w życie polityki bezpieczeństwa w odniesieniu do przetwarzania danych osobowych.*** W tym

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[28]. 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 incydentów***, które stanowią*** naruszenie danych osobowych, zmniejszając tym samym obciążenia administracyjne dla przedsiębiorstw i organów administracji publicznej.	kontekście właściwe organy***, pojedyncze punkty kontaktowe*** 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. Obowiązek zgłaszania incydentów zagrażających bezpieczeństwu ***należy wypełniać*** w sposób, który minimalizuje obciążenia administracyjne w przypadku, gdy incydent zagrażający bezpieczeństwu stanowi również naruszenie danych osobowych***, które wymaga zgłoszenia zgodnie z mającymi zastosowanie przepisami. ENISA powinna udzielić pomocy, opracowując*** mechanizmy wymiany informacji ***i jednolity wzór formularza***, ***które ułatwiłyby*** zgłaszanie incydentów ***stanowiących*** naruszenie danych osobowych, zmniejszając tym samym obciążenia administracyjne dla przedsiębiorstw i organów administracji publicznej.

[28] SEC(2012) 72 final

Uzasadnienie

Dostosowanie do projektu dyrektywy o ochronie danych.

Poprawka 30

Wniosek dotyczący dyrektywy
Motyw 32

Tekst proponowany przez Komisję	*Poprawka*
(32) Normalizacja wymogów w zakresie bezpieczeństwa jest procesem napędzanym przez rynek. W celu zapewnienia spójnego stosowania norm bezpieczeństwa państwa członkowskie powinny wspierać dążenie do zgodności lub zbieżności z określonymi	(32) Normalizacja wymogów w zakresie bezpieczeństwa jest ***dobrowolnym*** procesem napędzanym przez rynek***, który powinien umożliwić podmiotom gospodarczym korzystanie z alternatywnych środków w celu***

normami w celu zapewnienia wysokiego poziomu bezpieczeństwa na poziomie Unii. W tym celu ***konieczne*** może być przygotowanie ujednoliconych norm, czego należy dokonać zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniającym dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylającym decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE[29].

[29] Dz.U. L 316 z 14.11.2012, s. 12.

osiągnięcia co najmniej podobnych wyników. W celu zapewnienia spójnego stosowania norm bezpieczeństwa państwa członkowskie powinny wspierać dążenie do zgodności lub zbieżności z określonymi ***interoperacyjnymi*** normami w celu zapewnienia wysokiego poziomu bezpieczeństwa na poziomie Unii. W tym celu ***należy rozważyć stosowanie otwartych norm międzynarodowych do bezpieczeństwa sieci i informacji lub opracowanie takich narzędzi. Kolejnym koniecznym krokiem naprzód*** może być przygotowanie ujednoliconych norm, czego należy dokonać zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniającym dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylającym decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE[29]. ***W szczególności należy upoważnić ETSI, CEN i CENELEC do proponowania skutecznych i wydajnych otwartych norm bezpieczeństwa UE, w których unika się preferencji technologicznych w jak najwyższym stopniu i którymi mogą łatwo zarządzać małe i średnie podmioty gospodarcze. Normy międzynarodowe dotyczące bezpieczeństwa cybernetycznego należy dokładnie sprawdzić w celu zapewnienia, że nie zostały one naruszone, ustanawiają odpowiednie poziomy bezpieczeństwa, tym samym gwarantując, że zalecona zgodność z normami bezpieczeństwa cybernetycznego zwiększa, a nie zmniejsza ogólny poziom tego bezpieczeństwa w Unii.***

[29] Dz.U. L 316 z 14.11.2012, s. 12.

Poprawka 31

Wniosek dotyczący dyrektywy
Motyw 33

Tekst proponowany przez Komisję	*Poprawka*
(33) Komisja powinna okresowo dokonywać przeglądu niniejszej dyrektywy, w szczególności w celu sprawdzenia, czy konieczne jest wprowadzenie zmian w świetle zmieniających się technologii i warunków rynkowych.	(33) Komisja powinna okresowo dokonywać przeglądu niniejszej dyrektywy, ***w porozumieniu ze wszystkimi zainteresowanymi stronami,*** w szczególności w celu sprawdzenia, czy konieczne jest wprowadzenie zmian w świetle zmieniających się technologii i warunków ***społecznych, politycznych lub*** rynkowych.

Poprawka 32

Wniosek dotyczący dyrektywy
Motyw 34

Tekst proponowany przez Komisję	*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 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.	***skreślony***

Poprawka 33

Wniosek dotyczący dyrektywy
Motyw 35

Tekst proponowany przez Komisję	*Poprawka*
(35) Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, ***w tym*** na poziomie ekspertów. ***Przygotowując i opracowując akty delegowane,*** Komisja powinna zapewnić jednoczesne, terminowe i odpowiednie przekazywanie stosownych dokumentów Parlamentowi Europejskiemu i Radzie.	(35) Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje ***obejmujące wszystkie zainteresowane strony***, ***a w szczególności*** na poziomie ekspertów. Komisja powinna zapewnić jednoczesne, terminowe i odpowiednie przekazywanie stosownych dokumentów Parlamentowi Europejskiemu i Radzie.

Poprawka 34

Wniosek dotyczący dyrektywy
Motyw 36

Tekst proponowany przez Komisję	*Poprawka*
(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	(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 zbioru norm wzajemnych połączeń i bezpieczeństwa na rzecz*** 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 ***powiadamiania*** o ***znaczących*** incydentach. 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

przez Komisję[30].

[30] Dz.U. L 55 z 28.2.2011, s. 13.

członkowskie wykonywania uprawnień wykonawczych przez Komisję[30].

[30] Dz.U. L 55 z 28.2.2011, s. 13.

Poprawka 35

Wniosek dotyczący dyrektywy
Motyw 37

Tekst proponowany przez Komisję	*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 i opieki zdrowotnej.	(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 ***administracji elektronicznej,*** energetyki, transportu i opieki zdrowotnej.

Poprawka 36

Wniosek dotyczący dyrektywy
Motyw 38

Tekst proponowany przez Komisję	*Poprawka*
(38) Informacjami, które właściwy organ uznaje za poufne zgodnie z unijnymi i krajowymi przepisami dotyczącymi tajemnicy handlowej, można się wymieniać z Komisją ***i*** innymi właściwymi organami tylko wtedy, gdy wymiana taka jest absolutnie niezbędna w celu wykonania niniejszej dyrektywy. Ujawnione informacje powinny ograniczać się do tego, co jest właściwe i proporcjonalne do celów takiej wymiany informacji.	(38) Informacjami, które właściwy organ ***lub pojedynczy punkt kontaktowy*** uznaje za poufne zgodnie z unijnymi i krajowymi przepisami dotyczącymi tajemnicy handlowej, można się wymieniać z Komisją ***jej odpowiednimi agencjami,*** innymi ***pojedynczymi punktami kontaktowymi lub innymi*** właściwymi organami ***krajowymi*** tylko wtedy, gdy wymiana taka jest absolutnie niezbędna w celu wykonania niniejszej dyrektywy. Ujawnione informacje powinny ograniczać się do tego, co jest właściwe***, konieczne*** i proporcjonalne do celów takiej wymiany informacji***, a jednocześnie należy***

przestrzegać uprzednio ustalonych kryteriów dotyczących protokołów poufności, bezpieczeństwa i klasyfikacji regulujących wymianę informacji.

Poprawka 37

Wniosek dotyczący dyrektywy
Motyw 39

Tekst proponowany przez Komisję	*Poprawka*
(39) Wymiana informacji dotyczących zagrożeń i incydentów w ramach sieci współpracy i zapewnienie zgodności z wymogami dotyczącymi zgłaszania incydentów właściwym organom krajowym mogą oznaczać konieczność przetwarzania danych osobowych. Takie przetwarzanie danych osobowych jest niezbędne do realizacji celów niniejszej dyrektywy będących w interesie publicznym i w związku z tym jest uzasadnione na mocy art. 7 dyrektywy 95/46/WE. Nie stanowi ono, w odniesieniu do tych uzasadnionych celów, nieproporcjonalnej i niedopuszczalnej ingerencji naruszającej istotę prawa do ochrony danych osobowych, które gwarantuje art. 8 Karty praw podstawowych Unii Europejskiej. Przy wdrażaniu niniejszej dyrektywy zastosowanie powinno mieć, w stosownych przypadkach, rozporządzenie (WE) nr 1049/2001 ***Parlamentu Europejskiego i Rady*** z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji[31]. W przypadku gdy dane są przetwarzane przez instytucje i organy Unii, tego rodzaju przetwarzanie w celu wprowadzenia niniejszej dyrektywy w życie powinno być zgodne z rozporządzeniem (WE) nr 45/2001 ***Parlamentu Europejskiego i Rady*** z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem	(39) Wymiana informacji dotyczących zagrożeń i incydentów w ramach sieci współpracy i zapewnienie zgodności z wymogami dotyczącymi zgłaszania incydentów właściwym organom krajowym ***lub pojedynczym punktom kontaktowym*** mogą oznaczać konieczność przetwarzania danych osobowych. Takie przetwarzanie danych osobowych jest niezbędne do realizacji celów niniejszej dyrektywy będących w interesie publicznym i w związku z tym jest uzasadnione na mocy art. 7 dyrektywy 95/46/WE. Nie stanowi ono, w odniesieniu do tych uzasadnionych celów, nieproporcjonalnej i niedopuszczalnej ingerencji naruszającej istotę prawa do ochrony danych osobowych, które gwarantuje art. 8 Karty praw podstawowych Unii Europejskiej. Przy wdrażaniu niniejszej dyrektywy zastosowanie powinno mieć, w stosownych przypadkach, rozporządzenie ***Parlamentu Europejskiego i Rady*** (WE) nr 1049/2001 z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji[31]. W przypadku gdy dane są przetwarzane przez instytucje i organy Unii, tego rodzaju przetwarzanie w celu wprowadzenia niniejszej dyrektywy w życie powinno być zgodne z rozporządzeniem ***Parlamentu Europejskiego i Rady*** (WE) nr 45/2001 z dnia 18 grudnia 2000 r. o ochronie osób

danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych.

[31] Dz.U. L 145 z 31.5.2001, s. 43.

fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych.

[31] Dz.U. L 145 z 31.5.2001, s. 43.

Poprawka 38

Wniosek dotyczący dyrektywy
Motyw 41 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(41a) Zgodnie ze wspólną deklaracją polityczną państw członkowskich i Komisji dotyczącą dokumentów wyjaśniających z dnia 28 września 2011 r. państwa członkowskie zobowiązały się do złożenia, w uzasadnionych przypadkach, wraz z powiadomieniem o środkach transpozycji jednego lub więcej dokumentów wyjaśniających związki między elementami dyrektywy a odpowiadającymi im częściami krajowych instrumentów transpozycyjnych. W odniesieniu do niniejszej dyrektywy ustawodawca uznaje, że przekazanie takich dokumentów jest uzasadnione.

Poprawka 39

Wniosek dotyczący dyrektywy
Artykuł 1 – ustęp 2 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) ustanawia mechanizm współpracy między państwami członkowskimi w celu zapewnienia jednolitego stosowania niniejszej dyrektywy w obrębie Unii oraz, w razie konieczności, w celu zapewnienia skoordynowanego i sprawnego postępowania w przypadku wystąpienia zagrożeń i incydentów dotyczących sieci i	b) ustanawia mechanizm współpracy między państwami członkowskimi w celu zapewnienia jednolitego stosowania niniejszej dyrektywy w obrębie Unii oraz, w razie konieczności, w celu zapewnienia skoordynowanego i sprawnego postępowania w przypadku wystąpienia zagrożeń i incydentów dotyczących sieci i

systemów informatycznych oraz reagowania na nie;	systemów informatycznych oraz reagowania na nie***, z udziałem odpowiednich zainteresowanych stron***;

Poprawka 40

Wniosek dotyczący dyrektywy
Artykuł 1 – ustęp 6

Tekst proponowany przez Komisję	*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.	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 ***przekazywania zaufanym stronom trzecim i*** 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 przyjmują środki ustawodawcze zgodnie z art. 13 dyrektywy 95/46/WE, aby zagwarantować, że administracja publiczna, podmioty gospodarcze i właściwe organy nie będą uważane za odpowiedzialne za przetwarzanie danych osobowych koniecznych do wymiany informacji w ramach sieci współpracy i zgłaszania incydentów.***

Poprawka 41

Wniosek dotyczący dyrektywy
Artykuł 2 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
Państwa członkowskie mają prawo przyjmowania lub utrzymania w mocy	Państwa członkowskie mają prawo przyjmowania lub utrzymania w mocy

przepisów zapewniających wyższy poziom bezpieczeństwa, bez uszczerbku dla ich zobowiązań wynikających z prawa unijnego.	przepisów zapewniających wyższy poziom bezpieczeństwa ***zgodnie z Kartą praw podstawowych UE***, bez uszczerbku dla ich zobowiązań wynikających z prawa unijnego.

Uzasadnienie

Margines uznaniowości przyznany państwom członkowskim w zakresie bezpieczeństwa musi być podrzędny wobec poszanowania praw uznanych w Karcie praw podstawowych UE, a mianowicie, lecz nie tylko: prawa do poszanowania życia prywatnego i komunikowania się, prawa do ochrony danych osobowych, wolności prowadzenia działalności gospodarczej oraz prawa do skutecznego środka odwoławczego.

Poprawka 42

Wniosek dotyczący dyrektywy
Artykuł 3 – ustęp 1 – punkt 1 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) wszelkie urządzenia lub grupy połączonych lub powiązanych urządzeń, z których jedno lub więcej, zgodnie z oprogramowaniem, dokonuje automatycznego przetwarzania danych ***komputerowych***, jak również	b) wszelkie urządzenia lub grupy połączonych lub powiązanych urządzeń, z których jedno lub więcej, zgodnie z oprogramowaniem, dokonuje automatycznego przetwarzania danych ***cyfrowych***, jak również

Poprawka 43

Wniosek dotyczący dyrektywy
Artykuł 3 – ustęp 1 – punkt 1 – litera c

Tekst proponowany przez Komisję	*Poprawka*
c) dane ***komputerowe*** przechowywane, przetwarzane, odzyskiwane lub przekazywane przez elementy określone w lit. a) i b) w celu ich eksploatacji, użycia, ochrony lub utrzymania;	c) dane ***cyfrowe*** przechowywane, przetwarzane, odzyskiwane lub przekazywane przez elementy określone w lit. a) i b) w celu ich eksploatacji, użycia, ochrony lub utrzymania;

Poprawka 44

Wniosek dotyczący dyrektywy
Artykuł 3 – ustęp 1 – punkt 2

Tekst proponowany przez Komisję	*Poprawka*
2) „bezpieczeństwo” oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na zdarzenia przypadkowe lub działania złośliwe naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przekazywanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy;	2) „bezpieczeństwo” oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na zdarzenia przypadkowe lub działania złośliwe naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przekazywanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy; ***„bezpieczeństwo” w rozumieniu tej definicji obejmuje odpowiednie urządzenia techniczne, rozwiązania i procedury operacyjne spełniające wymogi bezpieczeństwa określone w niniejszej dyrektywie.***

Poprawka 45

Wniosek dotyczący dyrektywy
Artykuł 3 – ustęp 1 – punkt 4

Tekst proponowany przez Komisję	*Poprawka*
4) „incydent” oznacza każdą okoliczność lub zdarzenie, które ***mają*** rzeczywisty niekorzystny wpływ na bezpieczeństwo;	4) „incydent” oznacza każdą ***rozsądnie identyfikowalną*** okoliczność lub zdarzenie, które ***ma*** rzeczywisty niekorzystny wpływ na bezpieczeństwo;

Uzasadnienie

Pierwotne sformułowanie było zbyt szerokie i skomplikowałoby stosowanie tej definicji.

Poprawka 46

Wniosek dotyczący dyrektywy
Artykuł 3 – ustęp 1 – punkt 5

Tekst proponowany przez Komisję	*Poprawka*
5) „usługi społeczeństwa informacyjnego” oznaczają usługę w rozumieniu art. 1 pkt 2) dyrektywy 98/34/WE;	***skreślony***

Poprawka 47

Wniosek dotyczący dyrektywy
Artykuł 3 – ustęp 1 – 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;	***skreślony***

Poprawka 48

Wniosek dotyczący dyrektywy
Artykuł 3 – ustęp 1 – punkt 7

Tekst proponowany przez Komisję	*Poprawka*
7) „postępowanie w przypadku incydentu” oznacza wszystkie procedury umożliwiające analizę i ograniczenie skutków ***incydentu*** oraz reakcję na niego;	7) „postępowanie w przypadku incydentu” oznacza wszystkie procedury umożliwiające ***wykrycie incydentu, zapobieżenie mu, jego*** analizę i ograniczenie ***jego*** skutków oraz reakcję na niego;

Poprawka 49

Wniosek dotyczący dyrektywy
Artykuł 3 – ustęp 1 – punkt 8

Tekst proponowany przez Komisję	*Poprawka*
a) dostawcę usług społeczeństwa informacyjnego umożliwiających świadczenie innych usług społeczeństwa informacyjnego, których niewyczerpujący wykaz zamieszczony jest w załączniku II;	
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.	b) ***publicznego lub prywatnego*** operatora infrastruktury, która ma zasadnicze znaczenie dla utrzymania kluczowych działań gospodarczych i społecznych w dziedzinach energetyki, transportu, bankowości, ***rynków finansowych*** i opieki zdrowotnej, ***a której uszkodzenie lub zniszczenie miałoby poważny negatywny wpływ na dane państwo członkowskie w postaci braku możliwości utrzymania tych funkcji.*** Wykaz ***podmiotów gospodarczych*** zamieszczony jest w załączniku II.

Poprawka 50

Wniosek dotyczący dyrektywy
Artykuł 3 – ustęp 1 – punkt 8 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	8a) „incydent mający znaczące konsekwencje" oznacza incydent mający wpływ na bezpieczeństwo i ciągłość sieci informatycznej lub systemu informatycznego, który prowadzi do poważnego zakłócenia istotnych funkcji gospodarczych lub społecznych;

Poprawka 51

Wniosek dotyczący dyrektywy
Artykuł 3 – ustęp 1 – punkt 8 b (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	8b) „usługa” oznacza usługę świadczoną przez podmiot gospodarczy, z wyłączeniem wszelkich pozostałych usług tej samej jednostki;

Poprawka 52

Wniosek dotyczący dyrektywy
Artykuł 3 – ustęp 1 – punkt 11 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	11a) „rynek regulowany” oznacza rynek regulowany w rozumieniu art. 4 pkt 14 dyrektywy 2004/39/WE Parlamentu Europejskiego i Rady[28a];
	[28a] Dyrektywa 2004/39/WE Parlamentu Europejskiego i Rady z dnia 21 kwietnia 2004 r. w sprawie rynków instrumentów finansowych (Dz.U. L 45 z 16.2.2005, s. 18).

Poprawka 53

Wniosek dotyczący dyrektywy
Artykuł 3 – ustęp 1 – punkt 11 b (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	11b) „wielostronna platforma obrotu (MTF)” oznacza wielostronną platformę obrotu w rozumieniu art. 4 pkt 15 dyrektywy 2004/39/WE;

Poprawka 54

Wniosek dotyczący dyrektywy
Artykuł 3 – ustęp 1 – punkt 11 c (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	11c) „zorganizowana platforma obrotu" oznacza wielostronny system lub wielostronną platformę, niebędące rynkiem regulowanym, wielostronną platformą obrotu ani centralnym kontrahentem, obsługiwane przez przedsiębiorstwo inwestycyjne lub podmiot gospodarczy, w ramach których umożliwia się wzajemne powiązanie w obrębie systemu interesów licznych stron trzecich w zakresie kupna i sprzedaży obligacji, strukturyzowanych produktów finansowych, uprawnień do emisji lub instrumentów pochodnych w sposób skutkujący zawarciem kontraktu, zgodnie z przepisami tytułu II dyrektywy 2004/38/WE;

Poprawka 55

Wniosek dotyczący dyrektywy
Artykuł 4 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
Państwa członkowskie zapewniają wysoki poziom bezpieczeństwa sieci i systemów informatycznych na swoim terytorium zgodnie z niniejszą dyrektywą.	Państwa członkowskie zapewniają ***trwały, nieprzerwanie*** wysoki poziom bezpieczeństwa sieci i systemów informatycznych na swoim terytorium zgodnie z ***Kartą praw podstawowych Unii Europejskiej i z*** niniejszą dyrektywą.

Uzasadnienie

Zakres uznania udzielony państwom członkowskim w zakresie bezpieczeństwa musi być podrzędny wobec poszanowania praw uznanych w Karcie praw podstawowych UE, a mianowicie, lecz nie tylko, prawa do poszanowania życia prywatnego i komunikowania się, prawa do ochrony danych osobowych, wolności prowadzenia działalności gospodarczej oraz prawa do skutecznego środka odwoławczego.

Poprawka 56

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

Tekst proponowany przez Komisję	*Poprawka*
	ea) Państwa członkowskie mogą zwrócić się do Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) o pomoc w opracowywaniu krajowych strategii w zakresie bezpieczeństwa sieci i informacji oraz krajowych planów współpracy w zakresie bezpieczeństwa sieci i informacji na podstawie wspólnej minimalnej strategii w zakresie bezpieczeństwa sieci i informacji oraz projektu współpracy.

Poprawka 57

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 obejmujących*** określenie zagrożeń***, ustalenie stopnia ich ważności, ich ocenę*** i ***postępowanie w przypadku ich wystąpienia,*** ocenę wpływu potencjalnych incydentów***, sposoby zapobiegania i kontroli oraz kryteria wyboru możliwych środków zaradczych***;

Poprawka 58

Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 2 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) określenie funkcji i zakresu obowiązków poszczególnych podmiotów zaangażowanych ***w realizację planu***;	b) określenie funkcji i zakresu obowiązków poszczególnych ***organów i innych*** podmiotów zaangażowanych ***we wdrażanie***

tych ram;

Poprawka 59

Wniosek dotyczący dyrektywy
Artykuł 6 – nagłówek

Tekst proponowany przez Komisję	*Poprawka*
Właściwy organ krajowy ds. bezpieczeństwa sieci i systemów informatycznych	***Właściwe organy krajowe i krajowe pojedyncze punkty kontaktowe*** ds. bezpieczeństwa sieci i systemów informatycznych

Poprawka 60

Wniosek dotyczący dyrektywy
Artykuł 6 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Każde państwo członkowskie wyznacza właściwy organ krajowy ds. bezpieczeństwa sieci i systemów informatycznych („***właściwy organ***”).	1. Każde państwo członkowskie wyznacza ***co najmniej jeden*** właściwy organ krajowy ds. bezpieczeństwa sieci i systemów informatycznych (***zwany dalej*** „***właściwym organem***”).

Poprawka 61

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 też krajowy organ, np. właściwy organ, jako pojedynczy 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.

Poprawka 62

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

Tekst proponowany przez Komisję	*Poprawka*
	2b. Właściwe organy i pojedynczy punkt kontaktowy tego samego państwa członkowskiego ściśle ze sobą współpracują w zakresie obowiązków określonych w niniejszej dyrektywie.

Poprawka 63

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

Tekst proponowany przez Komisję	*Poprawka*
	2c. Pojedynczy punkt kontaktowy zapewnia współpracę transgraniczną z innymi pojedynczymi punktami kontaktowymi.

Poprawka 64

Wniosek dotyczący dyrektywy
Artykuł 6 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Państwa członkowskie zapewniają właściwym organom odpowiednie zasoby techniczne, finansowe i ludzkie, aby mogły one skutecznie i efektywnie realizować powierzone im zadania w celu osiągnięcia celów niniejszej dyrektywy. Państwa członkowskie zapewniają skuteczną, efektywną i bezpieczną współpracę ***właściwych organów*** za pośrednictwem sieci, o której mowa w art. 8.	3. Państwa członkowskie zapewniają właściwym organom ***i pojedynczym punktom kontaktowym*** odpowiednie zasoby techniczne, finansowe i ludzkie, aby mogły one skutecznie i efektywnie realizować powierzone im zadania w celu osiągnięcia celów niniejszej dyrektywy. Państwa członkowskie zapewniają skuteczną, efektywną i bezpieczną współpracę ***pojedynczych punktów kontaktowych*** za pośrednictwem sieci, o

której mowa w art. 8.

Poprawka 65

Wniosek dotyczący dyrektywy
Artykuł 6 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
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.	4. Państwa członkowskie dopilnowują, by właściwe organy ***i pojedyncze punkty kontaktowe*** 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.

Poprawka 66

Wniosek dotyczący dyrektywy
Artykuł 6 – ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. W stosownych przypadkach ***właściwe organy konsultują się i współpracują*** z odpowiednimi krajowymi organami ścigania ***i z organami ochrony danych***.	5. ***Właściwe organy obowiązkowo konsultują się z organami ochrony danych i współpracują*** w stosownych przypadkach z odpowiednimi krajowymi organami ścigania.

Uzasadnienie

Istnienie jednego właściwego organu odpowiedzialnego za pełnienie funkcji kontrolnej na szczeblu krajowym bez współpracy z innym organem odgrywającym rolę przeciwwagi nie prowadzi do równowagi między ochroną bezpieczeństwa a ochroną wolności.

Poprawka 67

Wniosek dotyczący dyrektywy
Artykuł 6 – ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. W stosownych przypadkach właściwe	5. W stosownych przypadkach właściwe

organy konsultują się i współpracują z odpowiednimi krajowymi organami ścigania i z organami ochrony danych.	organy ***i pojedyncze punkty kontaktowe*** konsultują się i współpracują z odpowiednimi krajowymi organami ścigania i z organami ochrony danych.

Poprawka 68

Wniosek dotyczący dyrektywy
Artykuł 6 – ustęp 6

Tekst proponowany przez Komisję	*Poprawka*
6. Każde państwo członkowskie powiadamia niezwłocznie Komisję o wyznaczeniu ***właściwego organu***, o ***jego*** zadaniach i o wszelkich późniejszych zmianach ***dotyczących tego organu***. Każde państwo członkowskie podaje do publicznej wiadomości informację o wyznaczeniu ***swojego właściwego organu***.	6. Każde państwo członkowskie powiadamia niezwłocznie Komisję o wyznaczeniu ***właściwych organów i pojedynczego punktu kontaktowego***, o ***ich*** zadaniach i o ***dotyczących ich*** wszelkich późniejszych zmianach. Każde państwo członkowskie podaje do publicznej wiadomości informację o wyznaczeniu ***właściwych organów***.

Poprawka 69

Wniosek dotyczący dyrektywy
Artykuł 7 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Każde państwo członkowskie ustanawia zespół reagowania na incydenty komputerowe (zwany dalej „CERT"), odpowiedzialny za postępowanie w przypadku wystąpienia incydentów i zagrożeń według jasno określonej procedury, która jest zgodna z wymogami określonymi w załączniku I pkt 1. CERT może zostać ustanowiony w ramach właściwego organu.	1. Każde państwo członkowskie ustanawia ***przynajmniej jeden*** zespół reagowania na incydenty komputerowe (zwany dalej „CERT") ***dla każdego sektora określonego w załączniku II***, odpowiedzialny za postępowanie w przypadku wystąpienia incydentów i zagrożeń według jasno określonej procedury, która jest zgodna z wymogami określonymi w załączniku I pkt 1. CERT może zostać ustanowiony w ramach właściwego organu.

Poprawka 70

Wniosek dotyczący dyrektywy
Artykuł 7 – ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. CERT ***działa*** pod nadzorem właściwego organu, który regularnie dokonuje przeglądu stosowności ***jego*** zasobów, ***jego mandatu*** oraz skuteczności ***jego*** procedury postępowania w przypadku incydentów.	5. CERT ***działają*** pod nadzorem właściwego organu ***lub pojedynczego punktu kontaktowego***, który regularnie dokonuje przeglądu stosowności ***ich*** zasobów, ***mandatów*** oraz skuteczności ***ich*** procedury postępowania w przypadku incydentów.

Poprawka 71

Wniosek dotyczący dyrektywy
Artykuł 7 – ustęp 5 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	5a. Państwa członkowskie zapewniają CERT odpowiednie zasoby ludzkie i finansowe, aby mogły one czynnie uczestniczyć w międzynarodowych, a zwłaszcza unijnych, sieciach współpracy.

Poprawka 72

Wniosek dotyczący dyrektywy
Artykuł 7 – ustęp 5 – punkt 1 (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	1) CERT są uprawnione i zachęcane do inicjowania wspólnych ćwiczeń z innymi CERT, z CERT ze wszystkich państw członkowskich oraz z właściwymi instytucjami państw trzecich, a także z CERT instytucji wielonarodowych i międzynarodowych, takich jak NATO czy ONZ, oraz do udziału w takich wspólnych ćwiczeniach.

Poprawka 73

Wniosek dotyczący dyrektywy
Artykuł 7 – ustęp 5 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	5a. Państwa członkowskie mogą zwrócić się do Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) lub do innych państw członkowskich o pomoc w rozwijaniu krajowych CERT.

Poprawka 74

Wniosek dotyczący dyrektywy
Artykuł 8

Tekst proponowany przez Komisję	*Poprawka*
1. ***Właściwe organy*** i Komisja ustanawiają sieć („sieć współpracy") ***służącą do współpracy*** w zakresie przeciwdziałania zagrożeniom i incydentom dotyczącym sieci i systemów informatycznych.	1. ***Pojedyncze punkty kontaktowe, Europejska Agencja ds. Bezpieczeństwa Sieci*** i ***Informacji (ENISA) i*** Komisja ustanawiają sieć („sieć współpracy")***, w ramach której współpracują*** w zakresie przeciwdziałania zagrożeniom i incydentom dotyczącym sieci i systemów informatycznych.
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.	2. Sieć współpracy umożliwia stałą łączność między Komisją a ***pojedynczymi punktami kontaktowymi.*** Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA) wspiera sieć współpracy poprzez zapewnianie wiedzy specjalistycznej i doradztwa. ***W stosownych przypadkach sieć współpracy współpracuje z organami ochrony danych.***
3. W ramach sieci współpracy ***właściwe organy***:	3. W ramach sieci współpracy ***pojedyncze punkty kontaktowe***:
a) przekazują wczesne ostrzeżenia dotyczące zagrożeń i incydentów zgodnie z	a) przekazują wczesne ostrzeżenia dotyczące zagrożeń i incydentów zgodnie z

art. 10;	art. 10;
b) zapewniają skoordynowaną reakcję zgodnie z art. 11;	b) zapewniają skoordynowaną reakcję zgodnie z art. 11;
c) regularnie publikują na wspólnej stronie internetowej niemające poufnego charakteru informacje na temat aktualnych wczesnych ostrzeżeń i skoordynowanych reakcji;	c) regularnie publikują na wspólnej stronie internetowej niemające poufnego charakteru informacje na temat aktualnych wczesnych ostrzeżeń i skoordynowanych reakcji;
	ca) wspólnie omawiają i koordynują przyjmowane przez siebie środki dotyczące wymogów w zakresie bezpieczeństwa i zgłaszania incydentów, o których mowa w art. 14, oraz środki dotyczące wdrażania i egzekwowania, o których mowa w art. 15, a także uzgadniają wspólną wykładnię i spójne stosowanie;
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;	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;
e) wspólnie omawiają i oceniają, na wniosek państwa członkowskiego lub Komisji, skuteczność CERT, zwłaszcza w przypadku gdy ćwiczenia w zakresie bezpieczeństwa sieci i informacji przeprowadzane są na poziomie unijnym;	e) wspólnie omawiają i oceniają, na wniosek ***ENISA,*** państwa członkowskiego lub Komisji, skuteczność CERT, zwłaszcza w przypadku gdy ćwiczenia w zakresie bezpieczeństwa sieci i informacji przeprowadzane są na poziomie unijnym***, a także wdrażają środki służące zaradzeniu bez zbędnej zwłoki zidentyfikowanym słabym stronom***;
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;	f) współpracują i wymieniają się informacjami dotyczącymi wszystkich istotnych kwestii ***w zakresie bezpieczeństwa sieci i informacji*** z innymi właściwymi organami europejskimi, w szczególności w dziedzinach energetyki, transportu, bankowości, ***rynków finansowych*** i opieki zdrowotnej;

	fa) wspólnie omawiają i uzgadniają wspólną wykładnię, spójne stosowanie i harmonijne wdrażanie w Unii postanowień rozdziału IV;
g) wymieniają się informacjami i najlepszymi praktykami między sobą i z Komisją oraz udzielają sobie wzajemnie pomocy w budowaniu zdolności w zakresie bezpieczeństwa sieci i informacji;	g) wymieniają się informacjami i najlepszymi praktykami między sobą i z Komisją oraz udzielają sobie wzajemnie pomocy w budowaniu zdolności w zakresie bezpieczeństwa sieci i informacji;
h) regularnie organizują wzajemne oceny zdolności i gotowości;	h) regularnie organizują wzajemne oceny zdolności i gotowości;
i) organizują ćwiczenia w zakresie bezpieczeństwa sieci i informacji na poziomie unijnym oraz uczestniczą, w stosownych przypadkach, w międzynarodowych ćwiczeniach w zakresie bezpieczeństwa sieci i informacji**.**	i) organizują ćwiczenia w zakresie bezpieczeństwa sieci i informacji na poziomie unijnym oraz uczestniczą, w stosownych przypadkach, w międzynarodowych ćwiczeniach w zakresie bezpieczeństwa sieci i informacji***;***
	ia) aktywnie promują zaangażowanie podmiotów gospodarczych oraz omawiają z nimi informacje i wymieniają się informacjami.
	Komisja regularnie informuje sieć współpracy o badaniach dotyczących bezpieczeństwa oraz innych stosownych programach programu „Horyzont 2020”.
	3a. W razie potrzeby do udziału w działaniach sieci współpracy, o której mowa w ust. 3 lit. c), g), h) i i), zaprasza się właściwe organy administracji publicznej i podmioty gospodarcze.
	3b. W przypadku gdy sieć współpracy przekazuje sobie lub ujawnia informacje, wczesne ostrzeżenia lub najlepsze praktyki pochodzące od podmiotów gospodarczych lub organów administracji publicznej, taka wymiana lub ujawnienie muszą być zgodne z klasyfikacją informacji ustaloną ze względu na jej pierwotne źródło zgodnie z art. 9 ust. 1.
	3c. Komisja publikuje raz w roku sprawozdanie z poprzednich 12 miesięcy, oparte na działalności sieci i na sprawozdaniu podsumowującym przekazanym zgodnie z art. 14 ust. 4

	niniejszej dyrektywy. Decyzje o informowaniu społeczeństwa o wszystkich poszczególnych incydentach zgłoszonych właściwym organom i pojedynczym punktom kontaktowym 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 podmioty gospodarcze, które zgłosiły te incydenty; może to nastąpić wyłącznie po uprzednich konsultacjach.
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, o której mowa w ust. 2 i 3***, pomiędzy pojedynczymi punktami kontaktowymi, ENISA i Komisją***. Te akty wykonawcze przyjmuje się zgodnie z procedurą doradczą, o której mowa w art. 19 ust. 2.

Poprawka 75

Wniosek dotyczący dyrektywy
Artykuł 9 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Wymiana szczególnie chronionych i poufnych informacji w ramach sieci współpracy odbywa się za pośrednictwem bezpiecznej infrastruktury.	Wymiana szczególnie chronionych i poufnych informacji w ramach sieci współpracy odbywa się za pośrednictwem bezpiecznej infrastruktury ***obsługiwanej pod nadzorem ENISA***. ***Państwa członkowskie dbają, aby szczególnie chronione lub tajne informacje przekazane przez inne państwa lub Komisję nie były ujawniane państwom trzecim lub wykorzystywane niezgodnie z celem, na przykład do działań tajnych służb bądź podejmowania decyzji gospodarczych.***

Poprawka 76

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*** dotyczących określenia kryteriów, jakie ***państwo członkowskie*** musi spełnić, aby móc uczestniczyć w bezpiecznym systemie wymiany informacji, w odniesieniu do:	2. Komisja jest uprawniona do przyjęcia aktów ***wykonawczych*** zgodnie z art. ***19*** dotyczących określenia kryteriów, jakie musi spełnić ***pojedynczy punkt kontaktowy***, aby móc uczestniczyć w bezpiecznym systemie wymiany informacji, w odniesieniu do:

Poprawka 77

Wniosek dotyczący dyrektywy
Artykuł 9 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
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.	3. Komisja przyjmuje – w drodze aktów wykonawczych – ***wspólny zbiór norm wzajemnych połączeń i bezpieczeństwa, jakich musi przestrzegać pojedynczy punkt kontaktowy, aby mógł uczestniczyć w wymianie informacji***. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 19 ust. 3.

Poprawka 78

Wniosek dotyczący dyrektywy
Artykuł 10

Tekst proponowany przez Komisję	*Poprawka*
1. W ramach sieci współpracy ***właściwe organy*** lub Komisja wydają wczesne ostrzeżenia dotyczące zagrożeń i incydentów, które spełniają co najmniej jeden z następujących warunków:	1. W ramach sieci współpracy ***pojedyncze punkty kontaktowe*** lub Komisja wydają wczesne ostrzeżenia dotyczące zagrożeń i incydentów, które spełniają co najmniej jeden z następujących warunków:
a) ich skala szybko rośnie lub może szybko	

wzrosnąć;

b) ***przekraczają one lub mogą przekroczyć*** krajowe zdolności reagowania;	b) ***w ocenie pojedynczego punktu kontaktowego skala ryzyka bądź incydentu szybko rośnie lub może szybko wzrosnąć i potencjalnie przekracza*** krajowe zdolności reagowania;
c) ***mają one*** wpływ ***lub mogą mieć wpływ*** na więcej niż jedno państwo członkowskie.	c) ***w ocenie pojedynczego punktu kontaktowego lub Komisji dane zagrożenie lub incydent ma*** wpływ na więcej niż jedno państwo członkowskie.
2. Wraz z wczesnym ostrzeżeniem ***właściwe organy*** i Komisja przekazują wszelkie stosowne informacje będące w ich posiadaniu, które mogą być przydatne do oceny zagrożenia lub incydentu.	2. Wraz z wczesnym ostrzeżeniem ***pojedyncze punkty kontaktowe*** i Komisja przekazują ***bez zbędnej zwłoki*** wszelkie stosowne informacje będące w ich posiadaniu, które mogą być przydatne do oceny zagrożenia lub incydentu. ***Informacje uznane przez właściwy podmiot gospodarczy za niejawne lub poufne oraz tożsamość takiego podmiotu podaje się w zakresie niezbędnym do oceny ryzyka lub incydentu.***
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.	3. Na wniosek państwa członkowskiego lub z własnej inicjatywy Komisja może zwrócić się do państwa członkowskiego o przedstawienie istotnych informacji ***jawnych*** dotyczących określonego zagrożenia lub incydentu.
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.	4. W sytuacji gdy zachodzi podejrzenie, iż zagrożenie lub incydent będące przedmiotem wczesnego ostrzeżenia mają ***poważny*** charakter przestępczy, ***pojedyncze punkty kontaktowe*** lub Komisja ***nawiązują kontakt z krajowymi organami ds. cyberprzestępczości, aby umożliwić im bez zbędnej zwłoki współpracę i wymianę informacji z działającym*** przy Europolu ***Europejskim*** Centrum ds. Walki z Cyberprzestępczością.
	4a. Członkowie sieci współpracy nie ujawniają publicznie żadnych uzyskanych informacji dotyczących ryzyka i incydentów zgodnie z ust. 1 bez uzyskania uprzedniej zgody na takie działanie ze strony powiadamiającego pojedynczego

	punktu kontaktowego.
	4b. W sytuacji gdy zachodzi podejrzenie, iż zagrożenie lub incydent będące przedmiotem wczesnego ostrzeżenia stanowią poważne zagrożenie lub poważny incydent o charakterze technicznym transnarodowym, pojedyncze punkty kontaktowe lub Komisja powiadamiają ENISA.
5. Komisja jest uprawniona do przyjęcia aktów ***delegowanych*** zgodnie z art. ***18***, dotyczących sprecyzowania zagrożeń i incydentów prowadzących do wczesnych ostrzeżeń, o których mowa w ust. 1.	5. Komisja jest uprawniona do przyjęcia aktów ***wykonawczych*** zgodnie z art. ***19***, dotyczących sprecyzowania zagrożeń i incydentów prowadzących do wczesnych ostrzeżeń, o których mowa w ust. 1***, a także procedur dzielenia się informacjami szczególnie chronionymi z punktu widzenia podmiotów gospodarczych***.

Poprawka 79

Wniosek dotyczący dyrektywy
Artykuł 11 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Po otrzymaniu wczesnego ostrzeżenia, o którym mowa w art. 10, ***właściwe organy*** – po przeanalizowaniu właściwych informacji – uzgadniają skoordynowaną reakcję zgodnie z unijnym planem współpracy w zakresie bezpieczeństwa sieci i informacji, o którym mowa w art. 12.	1. Po otrzymaniu wczesnego ostrzeżenia, o którym mowa w art. 10, ***pojedyncze punkty kontaktowe*** – po przeanalizowaniu właściwych informacji – uzgadniają ***bez zbędnej zwłoki*** skoordynowaną reakcję zgodnie z unijnym planem współpracy w zakresie bezpieczeństwa sieci i informacji, o którym mowa w art. 12.

Poprawka 80

Wniosek dotyczący dyrektywy
Artykuł 12 – ustęp 2 – litera a – tiret pierwsze

Tekst proponowany przez Komisję	*Poprawka*
– określenie formatu i procedur gromadzenia i wymiany kompatybilnych i porównywalnych informacji na temat zagrożeń i incydentów przez ***właściwe***	– określenie formatu i procedur gromadzenia i wymiany kompatybilnych i porównywalnych informacji na temat zagrożeń i incydentów przez ***pojedyncze***

organy;	***punkty kontaktowe***;

Poprawka 81

Wniosek dotyczący dyrektywy
Artykuł 12 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Unijny plan współpracy w zakresie bezpieczeństwa sieci i informacji przyjmuje się nie później niż jeden rok po wejściu w życie niniejszej dyrektywy i regularnie poddaje się go przeglądowi.	3. Unijny plan współpracy w zakresie bezpieczeństwa sieci i informacji przyjmuje się nie później niż jeden rok po wejściu w życie niniejszej dyrektywy i regularnie poddaje się go przeglądowi. ***Wyniki każdego przeglądu są przekazywane Parlamentowi Europejskiemu.***

Poprawka 82

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

Tekst proponowany przez Komisję	*Poprawka*
	3a. Komisja udostępnia budżet na opracowanie unijnego planu współpracy w zakresie bezpieczeństwa sieci i informacji.

Poprawka 83

Wniosek dotyczący dyrektywy
Artykuł 13 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
Bez uszczerbku dla możliwości podejmowania nieformalnej współpracy międzynarodowej przez sieć współpracy, Unia może zawierać umowy międzynarodowe z państwami trzecimi lub organizacjami międzynarodowymi,	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.	umożliwiając oraz organizując ich udział w określonych działaniach sieci współpracy. ***W umowach konieczne jest uwzględnienie procedury sprawdzającej, którą stosuje się w celu zagwarantowania*** ochrony danych osobowych ***przekazywanych*** w ramach sieci współpracy. ***O prowadzeniu negocjacji w sprawie umowy informuje się Parlament Europejski i zapewnia się jej przejrzystość. Każde przekazanie danych osobowych odbiorcom z siedzibą w krajach poza Unią odbywa się z zgodnie z art. 25 i 26 dyrektywy 95/46/WE oraz art. 9 rozporządzenia (WE) nr 45/2001.***

Uzasadnienie

Umowy międzynarodowe zawierane z innymi państwami lub z agencjami bezpieczeństwa powinny obowiązkowo uwzględniać instrument kontroli poszanowania praw obywatelskich. Ponadto Parlament Europejski powinien sprawować faktyczny nadzór demokratyczny nad umowami, a zatem powinien być we właściwym terminie informowany o przebiegu negocjacji w sprawie takich umów.

Poprawka 84

Wniosek dotyczący dyrektywy
Artykuł 14

Tekst proponowany przez Komisję	*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. Uwzględniając ***aktualny stan wiedzy i technologii***, środki ***te zapewniają*** poziom bezpieczeństwa stosowny do istniejącego zagrożenia. W szczególności należy ***podjąć*** środki zapobiegające incydentom ***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.

2. Państwa członkowskie ***dopilnowują***, aby ***organy administracji publicznej oraz*** podmioty gospodarcze zgłaszały ***właściwym organom*** incydenty mające ***znaczące*** konsekwencje dla bezpieczeństwa świadczonych przez nie usług podstawowych.

1. Państwa członkowskie zapewniają zastosowanie przez podmioty gospodarcze właściwych środków technicznych i organizacyjnych w celu ***wykrywania zagrożeń***, na jakie narażone są kontrolowane i wykorzystywane przez nie sieci i systemy informatyczne***, oraz skutecznego przeciwdziałania im***. Uwzględniając ***rozwój technologiczny***, ***te odpowiednie*** środki ***gwarantują*** poziom bezpieczeństwa stosowny do istniejącego zagrożenia. W szczególności należy ***przyjąć*** środki zapobiegające incydentom ***mającym wpływ na bezpieczeństwo*** sieci i systemów informatycznych oraz minimalizujące wpływ tych incydentów na świadczone przez nie podstawowe usługi, zapewniając tym samym ciągłość usług opartych na tych sieciach i systemach informatycznych.

2. Państwa członkowskie ***wdrażają mechanizmy w celu dopilnowania***, aby podmioty gospodarcze zgłaszały ***bez zbędnej zwłoki właściwemu organowi lub pojedynczemu punktowi kontaktowemu*** incydenty mające konsekwencje dla bezpieczeństwa ***lub ciągłości*** świadczonych przez nie usług podstawowych. ***Zgłoszenie nie może narażać strony zgłaszającej na większą odpowiedzialność. Aby określić znaczenie konsekwencji danego incydentu, uwzględnia się m.in. następujące parametry:***

a) liczbę użytkowników korzystających z usługi podstawowej, na którą ma wpływ dany incydent;

b) czas trwania incydentu;

c) zasięg geograficzny związany z obszarem, którego dotyczy incydent.

Kryteria te są określane bardziej szczegółowo zgodnie z art. 8 ust. 3 lit. ca) (nowa).

2a. Podmioty nieobjęte załącznikiem II

	mogą zgłaszać incydenty określone w art. 14 ust. 2 na zasadzie dobrowolności.
	2b. Odbiorca zgłoszenia o incydencie w możliwie krótkim terminie zdaje sprawę podmiotowi, który zgłosił incydent, o podjętych działaniach, decyzjach lub zaleceniach, jak również o powiadomieniu wszelkich stron trzecich oraz o protokołach dotyczących bezpieczeństwa i poufności regulujących wymianę informacji.
3. Wymogi zawarte w ust. 1 i 2 stosuje się do wszystkich podmiotów gospodarczych świadczących usługi w obrębie Unii Europejskiej.	3. Wymogi zawarte w ust. 1 i 2 stosuje się do wszystkich podmiotów gospodarczych świadczących usługi w obrębie Unii Europejskiej. ***Podmioty gospodarcze nieświadczące usług w Unii Europejskiej mogą zgłaszać incydenty na zasadzie dobrowolności.***
	3a. Państwa członkowskie zapewniają, aby podmioty gospodarcze zgłaszały incydenty, o których mowa w ust. 1 i 2, właściwemu organowi lub pojedynczemu punktowi kontaktowemu w państwie członkowskim, w którym incydent ma wpływ na podstawową usługę. Jeżeli incydent ma wpływ na usługi podstawowe w więcej niż jednym państwie członkowskim, pojedynczy punkt kontaktowy, który otrzymał zgłoszenie, alarmuje pozostałe zainteresowane pojedyncze punkty kontaktowe, opierając się na informacjach dostarczonych przez dany podmiot gospodarczy. Podmiotowi gospodarczemu przekazuje się w możliwie najkrótszym terminie informacje na temat innych pojedynczych punktów kontaktowych powiadomionych o incydencie, a także wszelkich podjętych kroków, rezultatów oraz wszelkie inne informacje mające znaczenie dla incydentu.
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***	4. ***Po konsultacji z właściwym organem i zainteresowanym podmiotem gospodarczym pojedynczy punkt kontaktowy informuje opinię publiczną o pojedynczych incydentach, jeżeli stwierdzi,***

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

że wiedza obywateli na ten temat jest niezbędna, by zapobiec incydentowi bądź uporać się z bieżącym incydentem, by umożliwić członkom społeczeństwa ograniczenie zagrożeń, na jakie sami są narażeni w związku z wystąpieniem incydentu, lub jeżeli podmiot gospodarczy, którego dotyczy incydent, odmówił niezwłocznego usunięcia poważnej strukturalnej usterki związanej z tym incydentem. Pojedynczy punkt kontaktowy należycie uzasadnia taką decyzję. Na ile to możliwe, właściwy organ ***lub pojedynczy punkt kontaktowy przedstawia podmiotom gospodarczym, które powiadomiły*** o incydencie***, informacje przeanalizowane pod kątem strategicznym, które pomogą przezwyciężyć zagrożenie dla bezpieczeństwa. Dwa razy*** do roku ***pojedynczy punkt kontaktowy*** przekazuje sieci współpracy sprawozdanie podsumowujące otrzymane zgłoszenia i działania podjęte zgodnie z niniejszym ustępem. ***Decyzje o informowaniu społeczeństwa o wszystkich poszczególnych incydentach zgłoszonych właściwym organom i pojedynczym punktom kontaktowym 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 podmioty gospodarcze, które zgłosiły te incydenty; może to nastąpić wyłącznie po uprzednich konsultacjach.***

W przypadku incydentów zgłaszanych sieci współpracy, o której mowa w art. 8, pozostałe właściwe organy krajowe nie podają do wiadomości publicznej żadnych uzyskanych informacji na temat zagrożeń lub incydentów bez zgody właściwego organu zgłaszającego.

5. Komisja jest uprawniona do przyjęcia aktów delegowanych zgodnie z art. 18 dotyczących określenia okoliczności, w

których organy administracji publicznej i podmioty gospodarcze są zobowiązane do zgłaszania incydentów.	
6. ***Z zastrzeżeniem wszelkich aktów delegowanych przyjętych na mocy ust. 5,*** właściwe organy ***mogą przyjąć*** wytyczne***, a w razie konieczności wydać instrukcje*** dotyczące okoliczności, w których ***organy administracji publicznej i*** podmioty gospodarcze są zobowiązane do zgłaszania incydentów.	6. Właściwe organy ***lub pojedyncze punkty kontaktowe przyjmują*** wytyczne dotyczące okoliczności, w których podmioty gospodarcze są zobowiązane do zgłaszania incydentów.
7. Komisja jest uprawniona do określenia – w drodze aktów wykonawczych – formatów i procedur mających zastosowanie do celów ust. 2. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 19 ust. 3.	7. Komisja jest uprawniona do określenia – w drodze aktów wykonawczych – formatów i procedur mających zastosowanie do celów ust. 2. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 19 ust. 3.
8. Ustępów 1 i 2 nie stosuje się w odniesieniu do mikroprzedsiębiorstw określonych w zaleceniu Komisji 2003/361/WE z dnia 6 maja 2003 r. w sprawie definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw[35].	8. Ustępów 1 i 2 nie stosuje się w odniesieniu do mikroprzedsiębiorstw określonych w zaleceniu Komisji 2003/361/WE z dnia 6 maja 2003 r. w sprawie definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw[35].
[35] Dz.U. L 124 z 20.5.2003, s. 36.	[35] Dz.U. L 124 z 20.5.2003, s. 36.

Poprawka 85

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 4 – akapit pierwszy (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	Podmioty gospodarcze zachęca się nie tylko do zgłaszania incydentów właściwemu organowi, lecz również do ogłaszania incydentów, polegającego na ich uwzględnianiu na zasadzie dobrowolności w swoich sprawozdaniach finansowych.

Uzasadnienie

Incydenty cybernetyczne mogą wiązać się z dużymi stratami finansowymi oraz ze znacznymi kosztami. Akcjonariusze i inwestorzy powinni być informowani o konsekwencjach tych incydentów. Zachęcając przedsiębiorstwa do podawania do wiadomości publicznej incydentów cybernetycznych na zasadzie dobrowolności można stymulować międzysektorową dyskusję na temat prawdopodobieństwa wystąpienia incydentów w przyszłości, wielkości takich zagrożeń, jak również słuszności działań zapobiegawczych podjętych w celu ograniczenia przypadków naruszania bezpieczeństwa cybernetycznego.

Poprawka 86

Wniosek dotyczący dyrektywy
Artykuł 15

Tekst proponowany przez Komisję	*Poprawka*
1. Państwa członkowskie zapewniają właściwym organom ***wszelkie*** uprawnienia niezbędne do ***badania przypadków niewypełniania przez organy administracji publicznej lub podmioty gospodarcze zobowiązań ciążących*** na ***nich na*** mocy art. 14 oraz ich wpływu na bezpieczeństwo sieci i systemów informatycznych.	1. Państwa członkowskie zapewniają właściwym organom ***i pojedynczym punktom kontaktowym*** uprawnienia niezbędne do ***zapewnienia zgodności z zobowiązaniami*** na mocy art. 14 oraz ich wpływu na bezpieczeństwo sieci i systemów informatycznych.
2. Państwa członkowskie zapewniają właściwym organom uprawnienia, na podstawie których mogą one wymagać od podmiotów gospodarczych ***i organów administracji publicznej***:	2. Państwa członkowskie zapewniają właściwym organom ***i pojedynczym punktom kontaktowym*** uprawnienia, na podstawie których mogą one wymagać od podmiotów gospodarczych:
a) przekazywania informacji potrzebnych do oceny bezpieczeństwa ich sieci i systemów informatycznych, w tym dokumentów dotyczących polityki w zakresie bezpieczeństwa;	a) przekazywania informacji potrzebnych do oceny bezpieczeństwa ich sieci i systemów informatycznych, w tym dokumentów dotyczących polityki w zakresie bezpieczeństwa;
b) ***poddania się audytowi*** bezpieczeństwa ***przeprowadzonemu*** przez wykwalifikowany niezależny podmiot lub organ krajowy oraz udostępnienia ***wyników tego audytu*** właściwemu organowi.	b) ***dostarczenia dowodów na skuteczną realizację strategii na rzecz*** bezpieczeństwa***, takich jak wyniki audytu bezpieczeństwa przeprowadzonego*** przez ***audytorów wewnętrznych,*** wykwalifikowany niezależny podmiot lub organ krajowy***,*** oraz udostępnienia ***tych dowodów*** właściwemu organowi ***lub pojedynczemu punktowi kontaktowemu***. ***W razie konieczności właściwy organ lub pojedynczy punkt kontaktowy może***

	zwrócić się o dodatkowe dowody lub – w drodze wyjątku i po przedstawieniu należytego uzasadnienia – przeprowadzić dodatkowy audyt.
	Kierując taki wniosek, właściwe organy i pojedyncze punkty kontaktowe podają cel wniosku i określają dokładnie, jakie informacje są wymagane.
3. Państwa członkowskie zapewniają właściwym organom uprawnienia do wydawania wiążących instrukcji dla podmiotów gospodarczych ***i organów administracji publicznej***.	3. Państwa członkowskie zapewniają właściwym organom ***i pojedynczym punktom kontaktowym*** uprawnienia do wydawania wiążących instrukcji dla ***wszystkich*** podmiotów gospodarczych ***określonych w załączniku II***.
4. Właściwe organy ***zgłaszają organom*** ścigania ***poważne incydenty***, które mogą mieć charakter przestępczy.	4. Właściwe organy ***i pojedyncze punkty kontaktowe informują zainteresowane podmioty gospodarcze o możliwości wniesienia do organów*** ścigania ***zarzutu popełnienia przestępstwa w przypadku poważnych incydentów***, które mogą mieć charakter przestępczy.
5. W przypadku incydentów prowadzących do naruszeń danych osobowych właściwe organy działają w ścisłej współpracy z organami ochrony danych osobowych.	5. ***Bez uszczerbku dla mającego zastosowanie prawa o ochronie danych,*** 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 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 95/46 Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych.***
	Komisja może przyjąć w drodze aktów wykonawczych, biorąc w jak najszerszym zakresie pod uwagę wszelkie mechanizmy wymiany informacji i jednolity wzór formularza opracowany przez pojedynczy punkt kontaktowy i organy ochrony

	danych we współpracy z ENISA, procedury dla mechanizmów wymiany informacji i format jednolitego wzoru formularza.
6. Państwa członkowskie zapewniają możliwość poddania kontroli sądowej wszelkich obowiązków nałożonych na ***organy administracji publicznej oraz*** podmioty gospodarcze na mocy niniejszego rozdziału.	6. Państwa członkowskie zapewniają możliwość poddania kontroli sądowej wszelkich obowiązków nałożonych na podmioty gospodarcze na mocy niniejszego rozdziału.

Poprawka 87

Wniosek dotyczący dyrektywy
Artykuł 16

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***, nie zalecając stosowania określonej technologii,*** wspierają stosowanie ***otwartych interoperacyjnych*** norm lub specyfikacji ***unijnych i międzynarodowych*** mających znaczenie dla bezpieczeństwa sieci i informacji***, zgodnych z prawodawstwem UE***.
2. Komisja ***sporządza – w drodze aktów wykonawczych – wykaz*** norm, o których mowa w ust. 1. Wykaz ten zostaje opublikowany w Dzienniku Urzędowym Unii Europejskiej.	2. Komisja ***nadaje odpowiedniemu organowi normalizacji europejskiej mandat do sporządzenia – w konsultacji z odpowiednimi zainteresowanymi stronami – wykazu*** norm ***lub specyfikacji***, o których mowa w ust. 1. Wykaz ten zostaje opublikowany w Dzienniku Urzędowym Unii Europejskiej.

Poprawka 88

Wniosek dotyczący dyrektywy
Artykuł 17 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Państwa członkowskie ustanawiają	1. Państwa członkowskie ustanawiają

przepisy o sankcjach mających zastosowanie, gdy naruszone zostaną krajowe przepisy przyjęte na podstawie niniejszej dyrektywy, i stosują wszelkie niezbędne środki, aby zapewnić ich wykonanie. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające. Najpóźniej w dniu, w którym przypada termin transpozycji niniejszej dyrektywy, państwa członkowskie powiadamiają Komisję o tych przepisach, a następnie niezwłocznie powiadamiają ją o wszelkich zmianach mających wpływ na te przepisy.	przepisy o sankcjach mających zastosowanie, gdy ***wskutek zaniedbania lub umyślnie*** naruszone zostaną krajowe przepisy przyjęte na podstawie niniejszej dyrektywy, i stosują wszelkie niezbędne środki, aby zapewnić ich wykonanie. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające. Najpóźniej w dniu, w którym przypada termin transpozycji niniejszej dyrektywy, państwa członkowskie powiadamiają Komisję o tych przepisach, a następnie niezwłocznie powiadamiają ją o wszelkich zmianach mających wpływ na te przepisy.

Uzasadnienie

Powinno być jasne, że sankcje można stosować wyłącznie w związku z naruszeniami, w przypadku których podmioty gospodarcze nie przyjęły wszelkich środków, których przyjęcia można by od nich racjonalnie oczekiwać. Podmioty gospodarcze mogłyby w przeciwnym razie zniechęcić się do zgłaszania incydentów.

Poprawka 89

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

Tekst proponowany przez Komisję	*Poprawka*
	1a. Państwa członkowskie dopilnowują, by sankcje, o których mowa w ust. 1 niniejszego artykułu, miały zastosowanie wyłącznie w przypadkach, gdy podmiot gospodarczy nie wywiązał się z obowiązków przewidzianych w rozdziale IV celowo lub w wyniku rażącego zaniedbania.

Poprawka 90

Wniosek dotyczący dyrektywy
Artykuł 18

Tekst proponowany przez Komisję	*Poprawka*
Artykuł 18	***skreślony***
Wykonywanie przekazanych uprawnień	
1. Powierzenie Komisji uprawnień do przyjęcia aktów delegowanych podlega warunkom określonym w niniejszym artykule.	
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.	
3. Przekazanie uprawnień, o którym mowa w art. 9 ust. 2, art. 10 ust. 5 i art. 14 ust. 5, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna od następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej lub w określonym w tej decyzji późniejszym terminie. Nie wpływa ona na ważność jakichkolwiek już obowiązujących aktów delegowanych.	
4. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.	
5. Akt delegowany przyjęty na podstawie art. 9 ust. 2, art. 10 ust. 5 i art. 14 ust. 5 wchodzi w życie tylko wówczas, gdy Parlament Europejski albo Rada nie wyraziły sprzeciwu w terminie dwóch	

miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

Poprawka 91

Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
Komisja dokonuje ***okresowego*** przeglądu funkcjonowania niniejszej dyrektywy i składa Parlamentowi Europejskiemu i Radzie sprawozdania na ten temat. Pierwsze sprawozdanie należy przedłożyć nie później niż ***trzy*** lata po dacie transpozycji, o której mowa w art. 21. W tym celu Komisja może zwrócić się do państw członkowskich o bezzwłoczne dostarczenie informacji.	***Co trzy lata*** Komisja dokonuje przeglądu funkcjonowania niniejszej dyrektywy i składa Parlamentowi Europejskiemu i Radzie sprawozdania na ten temat. Pierwsze sprawozdanie należy przedłożyć nie później niż ***dwa*** lata po dacie transpozycji, o której mowa w art. 21. W tym celu Komisja może zwrócić się do państw członkowskich o bezzwłoczne dostarczenie informacji.

Uzasadnienie

Należy regularnie dokonywać przeglądu załącznika II i redagować go, tak aby na bieżąco uwzględniał zmieniające się zagrożenia i warunki w dziedzinie bezpieczeństwa cybernetycznego.

Poprawka 92

Wniosek dotyczący dyrektywy
Załącznik I – nagłówek 1

Tekst proponowany przez Komisję	*Poprawka*
Zespoły reagowania na incydenty komputerowe (CERT) – wymogi i zadania	*(Nie dotyczy polskiej wersji językowej).*

Poprawka 93

Wniosek dotyczący dyrektywy
Załącznik I – ustęp 1 – wprowadzenie

Tekst proponowany przez Komisję	*Poprawka*
Wymogi i zadania dla CERT są odpowiednio i jasno określone i umocowane w strategiach lub regulacjach krajowych. Obejmują one następujące elementy:	Wymogi i zadania dla ***zespołów*** CERT są odpowiednio i jasno określone i umocowane w strategiach lub regulacjach krajowych. Obejmują one następujące elementy: *(Ta poprawka odnosi się do całego tekstu załącznika I).*

Poprawka 94

Wniosek dotyczący dyrektywy
Załącznik I – ustęp 1 – punkt 1 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) CERT ***zapewnia*** wysoką dostępność swoich usług łączności poprzez unikanie pojedynczych punktów awarii oraz ***dysponuje*** różnymi kanałami, za pomocą których można się z ***nim*** skontaktować i za pomocą których ***on sam może*** się kontaktować z innymi. Ponadto kanały komunikacyjne są wyraźnie określone i dobrze znane wśród użytkowników CERT i wśród współpracujących partnerów.	a) CERT ***zapewniają*** wysoką dostępność swoich usług łączności poprzez unikanie pojedynczych punktów awarii oraz ***dysponują*** różnymi kanałami, za pomocą których ***zawsze*** można się z ***nimi*** skontaktować i za pomocą których ***one same mogą*** się kontaktować z innymi. Ponadto kanały komunikacyjne są wyraźnie określone i dobrze znane wśród użytkowników CERT i wśród współpracujących partnerów.

Poprawka 95

Wniosek dotyczący dyrektywy
Załącznik I – ustęp 1 – punkt 1 – litera c

Tekst proponowany przez Komisję	*Poprawka*
c) Biura CERT oraz wspierające systemy informatyczne są zlokalizowane w bezpiecznych miejscach.	c) Biura CERT oraz wspierające systemy informatyczne są zlokalizowane w bezpiecznych miejscach ***z zabezpieczonymi***

sieciowymi systemami informatycznymi.

Poprawka 96

Wniosek dotyczący dyrektywy
Załącznik I – ustęp 1 – punkt 2 – litera a – tiret pierwsze

Tekst proponowany przez Komisję	*Poprawka*
– monitorowanie incydentów na poziomie krajowym;	– ***wykrywanie i*** monitorowanie incydentów na poziomie krajowym;

Poprawka 97

Wniosek dotyczący dyrektywy
Załącznik I – ustęp 1 – punkt 2 – litera a – tiret piąte a (nowe)

Tekst proponowany przez Komisję	*Poprawka*
	– czynne uczestnictwo w unijnych i międzynarodowych sieciach współpracy CERT.

Poprawka 98

Wniosek dotyczący dyrektywy
Załącznik II

Tekst proponowany przez Komisję	*Poprawka*
Wykaz podmiotów gospodarczych	Wykaz podmiotów gospodarczych
1. Energetyka	1. Energetyka
	a) Sieć elektryczna
	– dostawcy
	– operatorzy systemów dystrybucyjnych oraz detaliści sprzedający energię elektryczną konsumentom końcowym
	– operatorzy systemów przesyłowych energii elektrycznej
	– podmioty działające na rynku energii

	elektrycznej
	b) Ropa naftowa
	– podmioty eksploatujące rurociągi przesyłowe i magazyny ropy naftowej
	– operatorzy instalacji służących do produkcji, rafinacji, przetwarzania, magazynowania i przesyłu ropy naftowej
	c) Sieć gazowa
	– dostawcy
	– operatorzy systemów dystrybucyjnych oraz detaliści sprzedający gaz konsumentom końcowym
	– operatorzy systemów przesyłowych gazu ziemnego, operatorzy systemu magazynowania i operatorzy systemów LNG
	– operatorzy instalacji służących do produkcji, rafinacji, przetwarzania, magazynowania i przesyłu gazu
	– podmioty działające na rynku gazu
2. Transport	2. Transport
	a) Transport drogowy
	(i) operatorzy zarządzający ruchem
	(ii) pomocnicze usługi logistyczne:
	– magazynowanie i składowanie
	– przeładunek oraz
	– pozostała działalność wspomagająca transport
	b) Transport kolejowy
	(i) koleje (zarządcy infrastruktury, przedsiębiorstwa zintegrowane oraz przedsiębiorstwa transportu kolejowego)
	(ii) operatorzy zarządzający ruchem
	(iii) pomocnicze usługi logistyczne:
	– magazynowanie i składowanie
	– przeładunek oraz
	– pozostała działalność wspomagająca

	transport
	c) Transport lotniczy
	(i) przewoźnicy lotniczy (przewozy towarowe i pasażerskie)
	(ii) porty lotnicze
	(iii) operatorzy zarządzający ruchem
	(iv) pomocnicze usługi logistyczne:
	– magazynowanie
	– przeładunek oraz
	– pozostała działalność wspomagająca transport
	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
	– przeładunek oraz
	– pozostała działalność wspomagająca transport
	2a. Usługi wodne
3. Bankowość: instytucje kredytowe zgodnie z art. 4 pkt 1 dyrektywy 2006/48/WE.	3. Bankowość: instytucje kredytowe zgodnie z art. 4 pkt 1 dyrektywy 2006/48/WE.
4. Infrastruktura rynków finansowych: ***giełdy papierów wartościowych*** i izby rozliczeniowe partnerów centralnych.	4. Infrastruktura rynków finansowych: ***rynki regulowane, wielostronne platformy obrotu, zorganizowane platformy obrotu, internetowe portale płatnicze*** i izby rozliczeniowe partnerów centralnych.
5. Służba zdrowia: punkty opieki zdrowotnej (w tym szpitale i prywatne kliniki) i inne podmioty świadczące usługi opieki zdrowotnej.	5. Służba zdrowia: punkty opieki zdrowotnej (w tym szpitale i prywatne kliniki) i inne podmioty świadczące usługi opieki zdrowotnej.

6. TIK: usługi chmur obliczeniowych wykorzystywane przez podmiot do świadczenia usług wymienionych w pkt 1–5.

Przeglądu niniejszego wykazu dokonuje się co 2 lata.

PROCEDURA

Tytuł	Wspólny wysoki poziom bezpieczeństwa sieci i informacji w obrębie Unii
Odsyłacze	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)
Komisja przedmiotowo właściwa Data ogłoszenia na posiedzeniu	IMCO 15.4.2013
Opinia wydana przez Data ogłoszenia na posiedzeniu	ITRE 15.4.2013
Procedura obejmująca zaangażowane komisje - data ogłoszenia na posiedzeniu	12.9.2013
Sprawozdawca(czyni) komisji opiniodawczej Data powołania	Pilar del Castillo Vera 23.5.2013
Rozpatrzenie w komisji	14.10.2013 4.11.2013
Data przyjęcia	16.12.2013
Wynik głosowania końcowego	+: 36 –: 5 0: 0
Posłowie obecni podczas głosowania końcowego	Amelia Andersdotter, Josefa Andrés Barea, Bendt Bendtsen, Fabrizio Bertot, Reinhard Bütikofer, Maria Da Graça Carvalho, Giles Chichester, Pilar del Castillo Vera, Christian Ehler, Vicky Ford, Adam Gierek, Norbert Glante, Robert Goebbels, Fiona Hall, Romana Jordan, Philippe Lamberts, Marisa Matias, Judith A. Merkies, Angelika Niebler, Jaroslav Paška, Vittorio Prodi, Miloslav Ransdorf, Herbert Reul, Teresa Riera Madurell, Paul Rübig, Amalia Sartori, Salvador Sedó i Alabart, Evžen Tošenovský, Claude Turmes, Marita Ulvskog, Vladimir Urutchev
Zastępca(y) obecny(i) podczas głosowania końcowego	Daniel Caspary, António Fernando Correia de Campos, Françoise Grossetête, Roger Helmer, Jolanta Emilia Hibner, Seán Kelly, Eija-Riitta Korhola, Holger Krahmer, Zofija Mazej Kukovič, Silvia-Adriana Ţicău, Lambert van Nistelrooij
Zastępca(y) (art. 187 ust. 2) obecny(i) podczas głosowania końcowego	María Auxiliadora Correa Zamora

15.1.2014

OPINIA KOMISJI WOLNOŚCI OBYWATELSKICH, SPRAWIEDLIWOŚCI I SPRAW WEWNĘTRZNYCH*

dla Komisji Rynku Wewnętrznego i Ochrony Konsumentów

w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Sprawozdawca komisji opiniodawczej: Carl Schlyter

ZWIĘZŁE UZASADNIENIE

Celem wniosku jest osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i informacji w UE. Sprawozdawca komisji opiniodawczej popiera cele wyznaczone we wniosku, zalecając poprawki, które zwiększą pewność prawa oraz wzmocnią gwarancje i ochronę osób i ich prywatności, tak aby zapewnić kontrolę obywateli nad własnymi danymi osobowymi oraz ich zaufanie do środowiska cyfrowego, a także stworzyć kulturę działania opartą na przeciwdziałaniu zagrożeniom i doskonaleniu wymiany informacji między podmiotami prywatnymi i publicznymi.

Zaproponowane poprawki obejmują wzmocnienie odniesienia do przepisów dotyczących ochrony danych, sprecyzowanie, że pojęcie „infrastruktura krytyczna” nie powinno obejmować sieci społecznościowych i sklepów z aplikacjami (zob. poprawka do wykazu w załączniku II) oraz zapewnienie przestrzegania zasady proporcjonalności przez podkreślenie obywatelskiego aspektu przedsięwzięcia: większość zakłóceń i powszechnych przyczyn awarii systemów to nie dokonywane przez terrorystów, przestępców lub zagranicznych szpiegów zamierzone ataki cybernetyczne, lecz nieumyślne błędy ludzkie i przyczyny naturalne. Jest niezwykle istotne, aby UE oddzieliła wdrażanie proponowanych przepisów od wszelkiej militaryzacji tego zagadnienia, nie zajmując się celami sektora bezpieczeństwa i nadzoru, a przy tym uwzględniając kontekst zglobalizowanego rynku cyfrowego.

Ważną kwestią pozostaje związek między systemem zgłaszania zaproponowanym tutaj a systemem zaproponowanym w ogólnym rozporządzeniu o ochronie danych oraz ich efektywne współistnienie, co stanowi jeden z powodów, dla których podkreślamy, że wszelkie przepisy UE dotyczące bezpieczeństwa cybernetycznego należy wprowadzać po przyjęciu ogólnego rozporządzenia o ochronie danych, a nie przedtem. Ponadto należy wziąć pod uwagę realne konsekwencje finansowe i administracyjne, w tym całkowite koszty społeczne, a nie tylko koszty dokonywania zgłoszeń. Firmy programistyczne, które tworzą

oprogramowanie pośledniej jakości, a tym samym oszczędzają pieniądze, narażając klientów na zagrożenia, nie mogą we wszystkich przypadkach podlegać ochronie na podstawie zawartego w warunkach użytkowania standardowego zapisu zwalniającego z odpowiedzialności za niesprawność ich oprogramowania. Należy wprowadzić środki zachęcające je do zapewnienia racjonalnego poziomu bezpieczeństwa. Wreszcie, należy sprecyzować kluczowe pojęcia i nie pozostawiać państwom członkowskim pola do interpretacji (dotyczy to np. sformułowań „organy administracji publicznej", „znaczące skutki" oraz konkretnej definicji „cyberprzestępczości").

POPRAWKI

Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych zwraca się do Komisji Rynku Wewnętrznego i Ochrony Konsumentów, jako do komisji przedmiotowo właściwej, o naniesienie w swoim sprawozdaniu następujących poprawek:

Poprawka 1

Wniosek dotyczący dyrektywy
Motyw 1

Tekst proponowany przez Komisję	*Poprawka*
(1) Sieci oraz systemy i usługi informatyczne pełnią w społeczeństwie istotną rolę. Ich niezawodność i bezpieczeństwo mają zasadnicze znaczenie dla działalności gospodarczej ***i*** dobrobytu społeczeństwa***, a w szczególności dla funkcjonowania rynku wewnętrznego***.	(1) Sieci oraz systemy i usługi informatyczne pełnią w społeczeństwie istotną rolę. Ich niezawodność i bezpieczeństwo mają zasadnicze znaczenie dla działalności gospodarczej***,*** dobrobytu społeczeństwa oraz dla komunikacji ***i wymiany między osobami, organizacjami społeczeństwa obywatelskiego i przedsiębiorstwami, a także dla ochrony i poszanowania życia prywatnego i danych osobowych***.

Poprawka 2

Wniosek dotyczący dyrektywy
Motyw 2

Tekst proponowany przez Komisję	*Poprawka*
(2) Skala i częstotliwość umyślnych lub przypadkowych incydentów w obszarze bezpieczeństwa stają się coraz większe	(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.	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. ***Istnieje rosnące przekonanie, że systemy kontroli są podatne na ataki cybernetyczne z wielu źródeł, w tym ze strony wrogich rządów, grup terrorystycznych i innych podmiotów włamujących się do systemu w złym zamiarze. Przemyślane i skoordynowane ataki mogą mieć poważne konsekwencje dla stabilności, wyników i aspektów gospodarczych tej infrastruktury.***

Poprawka 3

Wniosek dotyczący dyrektywy
Motyw 3

Tekst proponowany przez Komisję	*Poprawka*
(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.	(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 ***oraz dla komunikacji i wymiany między osobami, organizacjami społeczeństwa obywatelskiego i przedsiębiorstwami***.

Poprawka 4

Wniosek dotyczący dyrektywy
Motyw 3 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(3a) Zważywszy, że do awarii systemów najczęściej dochodzi nadal z przyczyn niezamierzonych, jak przyczyny naturalne lub błędy ludzkie, infrastruktura powinna być odporna zarówno na zamierzone, jak i niezamierzone zakłócenia, a operatorzy infrastruktury krytycznej powinni projektować systemy oparte na zasadzie odporności, które działają nawet w razie awarii innych systemów poza ich kontrolą.

Poprawka 5

Wniosek dotyczący dyrektywy
Motyw 6 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(6a) Należy bezwzględnie przyznać, że brak pewności jest nieodłącznym elementem złożonych systemów, na których polegamy. Wymaga to, by podmioty, które chronią daną organizację, i podmioty, które wyznaczają strategiczne kierunki jej działania, jednakowo pojmowały, co ma znaczenie krytyczne.

Poprawka 6

Wniosek dotyczący dyrektywy
Motyw 8

Tekst proponowany przez Komisję	*Poprawka*
(8) Przepisy niniejszej dyrektywy nie powinny naruszać przysługujących każdemu państwu członkowskiemu praw do wprowadzania niezbędnych środków w	(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.	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***, pod warunkiem że nie służy im to za pretekst do niewywiązywania się ze spoczywających na nich bardziej ogólnych zobowiązań w zakresie poszanowania ochrony życia prywatnego i danych osobowych***. Zgodnie z art. 346 TFUE żadne państwo członkowskie nie ma obowiązku udzielania informacji, których ujawnienie uznaje za sprzeczne z podstawowymi interesami jego bezpieczeństwa.

Poprawka 7

Wniosek dotyczący dyrektywy
Motyw 9

Tekst proponowany przez Komisję	*Poprawka*
(9) W celu osiągnięcia i utrzymania wspólnego wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych każde państwo członkowskie powinno posiadać krajową strategię w zakresie bezpieczeństwa sieci i informacji określającą cele strategiczne i konkretne działania, które należy wdrożyć. Na poziome krajowym należy opracować spełniające zasadnicze wymagania plany współpracy w zakresie bezpieczeństwa sieci i informacji, tak aby osiągnąć poziom zdolności reagowania umożliwiający skuteczną i sprawną współpracę na poziomach krajowym i unijnym w przypadku wystąpienia incydentów.	(9) W celu osiągnięcia i utrzymania wspólnego wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych każde państwo członkowskie powinno posiadać krajową strategię w zakresie bezpieczeństwa sieci i informacji określającą cele strategiczne i konkretne działania, które należy wdrożyć. Na poziome krajowym należy opracować spełniające zasadnicze wymagania plany współpracy w zakresie bezpieczeństwa sieci i informacji, tak aby osiągnąć poziom zdolności reagowania umożliwiający skuteczną i sprawną współpracę na poziomach krajowym i unijnym w przypadku wystąpienia incydentów***, przy poszanowaniu i ochronie życia prywatnego i danych osobowych***.

Poprawka 8

Wniosek dotyczący dyrektywy
Motyw 10

Tekst proponowany przez Komisję	*Poprawka*
(10) W celu umożliwienia skutecznego wprowadzenia w życie przepisów przyjętych zgodnie z niniejszą dyrektywą w każdym państwie członkowskim należy ustanowić lub wyznaczyć organ odpowiedzialny za koordynowanie kwestii związanych z bezpieczeństwem sieci i informacji oraz działający jako centralny punkt kontaktowy ds. współpracy transgranicznej na poziomie UE. Organom tym należy zapewnić wystarczające zasoby techniczne, finansowe i ludzkie, aby mogły one skutecznie i efektywnie realizować powierzone im zadania w celu osiągnięcia celów niniejszej dyrektywy.	(10) W celu umożliwienia skutecznego wprowadzenia w życie przepisów przyjętych zgodnie z niniejszą dyrektywą w każdym państwie członkowskim należy ustanowić lub wyznaczyć właściwy organ ***krajowy objęty nadzorem cywilnym, prowadzący działalność podlegającą pełnej demokratycznej kontroli w sposób przejrzysty,*** odpowiedzialny za koordynowanie kwestii związanych z bezpieczeństwem sieci i informacji oraz działający jako centralny punkt kontaktowy ds. współpracy transgranicznej na poziomie UE. Organom tym należy zapewnić wystarczające zasoby techniczne, finansowe i ludzkie, aby mogły one skutecznie i efektywnie realizować powierzone im zadania w celu osiągnięcia celów niniejszej dyrektywy.

Poprawka 9

Wniosek dotyczący dyrektywy
Motyw 14 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(14a) Coraz więcej sektorów – jak np. usługi IT przy obsłudze infrastruktury krytycznej – stosuje w swoim środowisku informatycznym usługi przetwarzania w chmurze obliczeniowej. Wystarczające środki bezpieczeństwa muszą zapewnić poufność, integralność i dostępność danych w chmurze. Usługi w zakresie infrastruktury serwerowej oraz przechowywania danych wrażliwych w chmurze obliczeniowej wiążą się z wymogami bezpieczeństwa i odporności, którym obecne usługi w chmurze

	obliczeniowej nie są w stanie sprostać. Dlatego należy uzyskać pewność, że środowisko przetwarzania w chmurze może zapewnić niezawodną ochronę wrażliwych danych dotyczących infrastruktury krytycznej.

Poprawka 10

Wniosek dotyczący dyrektywy
Motyw 15

Tekst proponowany przez Komisję	*Poprawka*
(15) Ponieważ większość sieci i systemów informatycznych eksploatowana jest przez podmioty prywatne, niezbędna jest współpraca między sektorem publicznym i prywatnym. Podmioty gospodarcze należy zachęcać do tworzenia własnych nieformalnych mechanizmów współpracy w celu zapewnienia bezpieczeństwa sieci i informacji. Powinny one również współpracować z sektorem publicznym oraz dzielić się z nim informacjami i najlepszymi praktykami ***w zamian za wsparcie operacyjne*** w przypadku incydentów.	(15) Ponieważ większość sieci i systemów informatycznych eksploatowana jest przez podmioty prywatne, niezbędna jest współpraca między sektorem publicznym i prywatnym. Podmioty gospodarcze należy zachęcać do tworzenia własnych nieformalnych mechanizmów współpracy w celu zapewnienia bezpieczeństwa sieci i informacji. Powinny one również współpracować z sektorem publicznym oraz dzielić się z nim informacjami i najlepszymi praktykami ***na zasadzie wzajemności, a przy tym należy zapewnić obustronne wsparcie operacyjne*** w przypadku incydentów.

Poprawka 11

Wniosek dotyczący dyrektywy
Motyw 15 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(15a) Istniejące już krajowe mechanizmy współpracy między podmiotami publicznymi i prywatnymi powinny być w pełni przestrzegane, w miarę możliwości i zgodnie z dyrektywą 95/46/WE, a przepisy niniejszej dyrektywy nie mogą mieć negatywnego wpływu na takie ustanowione rozwiązania w zakresie

współpracy.

Poprawka 12

Wniosek dotyczący dyrektywy
Motyw 16

Tekst proponowany przez Komisję	*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.	(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 ***na bieżąco wyczerpujące*** niemające poufnego charakteru informacje na temat incydentów i zagrożeń.

Poprawka 13

Wniosek dotyczący dyrektywy
Motyw 21

Tekst proponowany przez Komisję	*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.	(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***, pod warunkiem że państwa, z którymi współpraca ta jest przewidywana, posiadają instrumenty kontroli i ochrony danych zapewniające taki sam poziom bezpieczeństwa jak instrumenty unijne***.

Poprawka 14

Wniosek dotyczący dyrektywy
Motyw 22

Tekst proponowany przez Komisję	*Poprawka*
(22) Odpowiedzialność za zapewnienie bezpieczeństwa sieci i informacji w dużym stopniu spoczywa na organach administracji publicznej i ***podmiotach gospodarczych***. Za pomocą stosownych wymogów regulacyjnych i dobrowolnych praktyk branżowych należy wspierać i rozwijać kulturę przeciwdziałania zagrożeniom, obejmującą przeprowadzanie ocen zagrożenia i wdrażanie środków bezpieczeństwa ***stosownych do danego zagrożenia***. Stworzenie równych warunków działania ma również kluczowe znaczenie dla skutecznego funkcjonowania sieci współpracy w celu zapewnienia skutecznej współpracy ze strony wszystkich państw członkowskich.	(22) Odpowiedzialność za zapewnienie bezpieczeństwa sieci i informacji w dużym stopniu spoczywa na organach administracji publicznej i ***przedsiębiorstwach***. Za pomocą wymogów regulacyjnych i dobrowolnych praktyk branżowych należy wspierać i rozwijać kulturę przeciwdziałania zagrożeniom, obejmującą przeprowadzanie ocen zagrożenia i wdrażanie środków bezpieczeństwa ***mających na celu uprzedzanie umyślnych lub przypadkowych incydentów w obszarze bezpieczeństwa. Tam, gdzie taka kultura przeciwdziałania zagrożeniom już istnieje, a zwłaszcza tam, gdzie opiera się ona na dobrowolnej praktyce, powinna być wspierana, umacniana i propagowana.*** Stworzenie równych warunków działania ma również kluczowe znaczenie dla skutecznego funkcjonowania sieci współpracy w celu zapewnienia skutecznej współpracy ze strony wszystkich państw członkowskich.

Poprawka 15

Wniosek dotyczący dyrektywy
Motyw 22 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(22a) Organy administracji publicznej i przedsiębiorstwa prywatne – w tym dostawcy usług sieciowych i informacyjnych oraz oprogramowania – powinny postrzegać ochronę swoich systemów informatycznych i danych, które systemy te zawierają, jako część spoczywającego na nich obowiązku staranności. Należy zapewnić stosowne poziomy ochrony przed możliwym do racjonalnego rozpoznania zagrożeniem i narażeniem na zagrożenie. Koszty

	i ciężar takiej ochrony powinny odpowiadać szkodom, które prawdopodobnie zostałyby poniesione w wyniku ataku cybernetycznego przez jego ofiary.

Poprawka 16

Wniosek dotyczący dyrektywy
Motyw 26 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(26a) Dzieci mają do czynienia z internetem i innymi nowymi technologiami od wczesnych lat życia, a w konsekwencji są podatne na zagrożenia z nimi związane. Właściwe zarządzanie przyjazną dla dzieci przestrzenią internetową jest kluczowe, by ograniczyć szkody i nie dopuścić do zaniedbania ochrony dzieci i ich praw.

Poprawka 17

Wniosek dotyczący dyrektywy
Motyw 28

Tekst proponowany przez Komisję	*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***	(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 ***z uwzględnieniem pierwszeństwa interesu publicznego***, zgodnie z którym społeczeństwo powinno być informowane o zagrożeniach, ***nad krótkoterminowymi względami gospodarczymi***.

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.

Poprawka 18

Wniosek dotyczący dyrektywy
Motyw 29 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(29a) Korzystanie z internetu w sposób stanowiący nadużycie pozwala zorganizowanym grupom przestępczym na rozszerzanie działalności online w celach takich jak pranie pieniędzy, fałszerstwa oraz oferowanie innych produktów i usług naruszających prawo własności intelektualnej, a także na próby podejmowania nowych działań przestępczych, co pokazuje alarmującą zdolność do dostosowywania się do nowych technologii.

Poprawka 19

Wniosek dotyczący dyrektywy
Motyw 30 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(30a) Cyberprzestępczość powoduje coraz większe straty gospodarcze i społeczne, dotykając miliony konsumentów i przynosząc roczne straty szacowane na 290 mld EUR1[4a];
	[4a] Zgodnie z danymi przedstawionymi w Norton Cybercrime Report 2012.

Poprawka 20

Wniosek dotyczący dyrektywy
Motyw 33

Tekst proponowany przez Komisję	*Poprawka*
(33) Komisja powinna okresowo dokonywać przeglądu niniejszej dyrektywy, w szczególności w celu sprawdzenia, czy konieczne jest wprowadzenie zmian w świetle zmieniających się technologii i warunków rynkowych.	(33) Komisja powinna okresowo dokonywać przeglądu niniejszej dyrektywy, w szczególności w celu sprawdzenia, czy konieczne jest wprowadzenie zmian w świetle zmieniających się technologii i warunków rynkowych ***oraz obowiązków mających na celu zapewnienie najwyższego poziomu bezpieczeństwa i integralności sieci, a także informacji i ochrony życia prywatnego i danych osobowych***.

Poprawka 21

Wniosek dotyczący dyrektywy
Motyw 39

Tekst proponowany przez Komisję	*Poprawka*
(39) Wymiana informacji dotyczących zagrożeń i incydentów w ramach sieci współpracy i zapewnienie zgodności z wymogami dotyczącymi zgłaszania incydentów właściwym organom krajowym mogą oznaczać konieczność przetwarzania danych osobowych. Takie przetwarzanie danych osobowych jest niezbędne do realizacji celów niniejszej dyrektywy będących w interesie publicznym ***i w związku z tym jest*** uzasadnione na mocy art. 7 dyrektywy 95/46/WE. Nie ***stanowi*** ono***, w odniesieniu do tych uzasadnionych celów, nieproporcjonalnej i niedopuszczalnej ingerencji naruszającej istotę*** prawa do ochrony danych osobowych, które gwarantuje art. 8 Karty praw	(39) Wymiana informacji dotyczących zagrożeń i incydentów w ramach sieci współpracy i zapewnienie zgodności z wymogami dotyczącymi zgłaszania incydentów właściwym organom krajowym mogą oznaczać konieczność przetwarzania danych osobowych. ***Jeżeli*** takie przetwarzanie danych osobowych jest niezbędne do realizacji celów niniejszej dyrektywy będących w interesie publicznym***, może być ono*** uzasadnione na mocy art. 7 dyrektywy 95/46/WE. Nie ***zwalnia*** ono ***jednak właściwych organów z obowiązku proporcjonalnego działania w sposób w żadnym razie nienaruszający*** prawa do ochrony danych osobowych, które gwarantuje art. 8 Karty praw podstawowych Unii Europejskiej. Przy

podstawowych Unii Europejskiej. Przy wdrażaniu niniejszej dyrektywy zastosowanie powinno mieć, w stosownych przypadkach, rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji[31]. W przypadku gdy dane są przetwarzane przez instytucje i organy Unii, tego rodzaju przetwarzanie w celu wprowadzenia niniejszej dyrektywy w życie powinno być zgodne z rozporządzeniem (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.	wdrażaniu niniejszej dyrektywy zastosowanie powinno mieć, w stosownych przypadkach, rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji[31]. W przypadku gdy dane są przetwarzane przez instytucje i organy Unii, tego rodzaju przetwarzanie w celu wprowadzenia niniejszej dyrektywy w życie powinno być zgodne z rozporządzeniem (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.
[31] Dz.U. L 145 z 31.5.2001, s. 43.	[31] Dz.U. L 145 z 31.5.2001, s. 43.

Poprawka 22

Wniosek dotyczący dyrektywy
Motyw 41 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(41a) W przypadku wszystkich środków należy zagwarantować ochronę podstawowych praw człowieka, w szczególności praw określonych w Europejskiej konwencji praw człowieka (art. 8 – poszanowanie życia prywatnego), oraz zapewnić przestrzeganie zasady proporcjonalności.

Poprawka 23

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 ***jest w pełni zgodna z dyrektywą*** 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, ***dyrektywą*** 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. ***dotyczącą*** przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz ***rozporządzeniem (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.

Poprawka 24

Wniosek dotyczący dyrektywy
Artykuł 2

Tekst proponowany przez Komisję	*Poprawka*
Państwa członkowskie mają prawo przyjmowania lub utrzymania w mocy przepisów zapewniających wyższy poziom bezpieczeństwa, bez uszczerbku dla ich zobowiązań wynikających z prawa unijnego.	Państwa członkowskie mają prawo przyjmowania lub utrzymania w mocy przepisów zapewniających wyższy poziom bezpieczeństwa, bez uszczerbku dla ich zobowiązań wynikających z prawa unijnego***, przepisy takie muszą być jednak zgodne ze wspólnymi minimalnymi warunkami w tym zakresie, które są przewidziane w niniejszej dyrektywie***.

Poprawka 25

Wniosek dotyczący dyrektywy

Artykuł 3 – punkt 2

Tekst proponowany przez Komisję	*Poprawka*
(2) „bezpieczeństwo” oznacza odporność sieci i systemów informatycznych***, przy danym poziomie zaufania,*** na zdarzenia przypadkowe lub działania złośliwe naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przekazywanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy;	2) „bezpieczeństwo” oznacza odporność sieci i systemów informatycznych na zdarzenia przypadkowe lub działania złośliwe naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przekazywanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy;

Poprawka 26

Wniosek dotyczący dyrektywy
Artykuł 3 – ustęp 2 – litera a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	„odporność na zagrożenia cybernetyczne” oznacza zdolność sieci i systemów informacyjnych do oparcia się zagrożeniu i powrotu do pełnej zdolności operacyjnej po incydentach, w tym – między innymi – takich jak niesprawność techniczna, awaria zasilania lub incydenty dotyczące bezpieczeństwa;

Poprawka 27

Wniosek dotyczący dyrektywy
Artykuł 3 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
„incydent” oznacza każdą okoliczność lub zdarzenie, które mają rzeczywisty niekorzystny wpływ na bezpieczeństwo;	„incydent” oznacza każdą okoliczność lub zdarzenie, które mają rzeczywisty niekorzystny wpływ na bezpieczeństwo ***i świadczenie podstawowych usług***;

Poprawka 28

Wniosek dotyczący dyrektywy

Artykuł 3 – punkt 8 – litera b

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

Poprawka 29

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, które obejmują co najmniej regularną ocenę*** zagrożeń ***umożliwiającą*** określenie zagrożeń i ocenę wpływu potencjalnych incydentów ***oraz środki zapewniające bezpieczeństwo i integralność informacji, w tym środki szybkiego ostrzegania***;

Uzasadnienie

Plan oceny jest niewystarczający i nie zwiera innych środków niezbędnych do zarządzania ryzykiem w dziedzinie bezpieczeństwa sieci i informacji. EIOD zaleca wprowadzenie ram zarządzania ryzykiem, które obejmują ocenę zagrożeń.

Poprawka 30

Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. ***Krajową strategię*** w zakresie bezpieczeństwa sieci i informacji oraz krajowy plan współpracy w zakresie	3. ***Krajowa strategia*** 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.	bezpieczeństwa sieci i informacji są przekazywane Komisji***, Parlamentowi Europejskiemu, Radzie i Europejskiemu Inspektorowi Ochrony Danych*** w ciągu jednego miesiąca od ich przyjęcia***, które następuje nie później niż 12 miesięcy od wejścia w życie niniejszej dyrektywy***.

Poprawka 31

Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 3 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	3a. Komisja sporządza streszczenie strategii bezpieczeństwa sieci i informacji wszystkich państw członkowskich i przekazuje je wszystkim państwom członkowskim w uporządkowanej formie.

Uzasadnienie

Dla państw członkowskich przydatna będzie możliwość zapoznania się również z innymi planami. Pomoże im to określić ich własne podejście i może nawet stworzyć możliwość wymiany najlepszych praktyk.

Poprawka 32

Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 3 b (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	3b. W sześć miesięcy od przyjęcia niniejszej dyrektywy Komisja tworzy zestaw wytycznych dotyczących struktury strategii bezpieczeństwa sieci i informacji. Ma on ułatwić państwom członkowskim opracowywanie i przyjmowanie dokumentów posiadających podobną strukturę.

Uzasadnienie

Praca w zakresie organizacji i sporządzania streszczeń na szczeblu Wspólnoty może być

skuteczniejsza, jeżeli 28 dokumentów, na których będą się one opierać, będzie posiadało podobną ogólną strukturę. Pomimo że wytyczne Komisji nie byłyby wiążące, w konsekwencji skłaniałyby one jednak państwa członkowskie do stosowania zalecanego modelu/ struktury przy sporządzaniu strategii krajowych.

Poprawka 33

Wniosek dotyczący dyrektywy
Artykuł 6 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Każde państwo członkowskie wyznacza właściwy organ krajowy ds. bezpieczeństwa sieci i systemów informatycznych („właściwy organ”).	1. Każde państwo członkowskie wyznacza właściwy ***cywilny*** organ krajowy ds. bezpieczeństwa sieci i systemów informatycznych („właściwy organ”).

Poprawka 34

Wniosek dotyczący dyrektywy
Artykuł 6 – ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. ***W stosownych przypadkach*** właściwe organy konsultują się i współpracują z ***odpowiednimi*** krajowymi organami ścigania i z organami ochrony danych.	5. Właściwe organy konsultują się i ***ściśle*** współpracują z ***właściwymi*** krajowymi organami ścigania i z organami ochrony danych***, w stosownych przypadkach i z uwzględnieniem zasady proporcjonalności***.

Poprawka 35

Wniosek dotyczący dyrektywy
Artykuł 6 – ustęp 5 (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	5a. Właściwe organy spełniają – w odniesieniu do gromadzonych, przetwarzanych i wymienianych informacji – wymogi dotyczące ochrony danych osobowych określone w art. 17 dyrektywy 95/46/WE.

Poprawka 36

Wniosek dotyczący dyrektywy
Artykuł 7 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Każde państwo członkowskie ustanawia ***zespół*** reagowania na incydenty komputerowe (***zwany*** dalej „CERT"), ***odpowiedzialny*** za postępowanie w przypadku wystąpienia incydentów i zagrożeń według jasno określonej procedury, która jest zgodna z wymogami określonymi w załączniku I pkt 1. CERT ***może zostać*** ustanowiony w ramach właściwego organu.	1. Każde państwo członkowskie ustanawia ***zespoły*** reagowania na incydenty komputerowe (***zwane*** dalej „CERT"), ***odpowiedzialne*** za postępowanie w przypadku wystąpienia incydentów i zagrożeń według jasno określonej procedury, która jest zgodna z wymogami określonymi w załączniku I pkt 1. ***W stosownych przypadkach*** CERT ***zostaje*** ustanowiony w ramach właściwego organu.

Poprawka 37

Wniosek dotyczący dyrektywy
Artykuł 8 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
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***.	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 ***bezstronnego poradnictwa technicznego oraz właściwych środków w sektorze publicznym i prywatnym***.

Poprawka 38

Wniosek dotyczący dyrektywy
Artykuł 9 – ustęp 2 – litera b a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	ba) kryteriów udziału państw członkowskich w bezpiecznym systemie wymiany informacji w celu zagwarantowania wysokiego poziomu

	bezpieczeństwa i odporności 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.

Poprawka 39

Wniosek dotyczący dyrektywy
Artykuł 9 ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
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.	***skreślony***

Poprawka 40

Wniosek dotyczący dyrektywy
Artykuł 12 – ustęp 2 – litera a – tiret drugie

Tekst proponowany przez Komisję	*Poprawka*
– określenie ***procedur i*** kryteriów oceny zagrożeń i incydentów przez sieć współpracy;	– określenie kryteriów oceny zagrożeń i incydentów przez sieć współpracy;

Poprawka 41

Wniosek dotyczący dyrektywy
Artykuł 13

Tekst proponowany przez Komisję	*Poprawka*
Bez uszczerbku dla możliwości podejmowania nieformalnej współpracy międzynarodowej przez sieć współpracy,	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.	Unia może zawierać umowy międzynarodowe z państwami trzecimi lub organizacjami międzynarodowymi, umożliwiając oraz organizując ich udział w określonych działaniach sieci współpracy. Takie umowy ***są zawierane jedynie wtedy, gdy zapewniony może być wystarczający i porównywalny z unijnym poziom*** ochrony danych osobowych, które są przekazywane w ramach sieci współpracy.

Poprawka 42

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 1

Tekst proponowany przez Komisję	*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. Uwzględniając aktualny stan wiedzy i technologii, środki te zapewniają poziom bezpieczeństwa stosowny do istniejącego zagrożenia. W szczególności należy podjąć środki zapobiegające incydentom 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.	1. Państwa członkowskie zapewniają zastosowanie przez organy administracji publicznej i podmioty gospodarcze właściwych środków technicznych i organizacyjnych w celu ***wykrywania zagrożeń***, na jakie narażone są kontrolowane i wykorzystywane przez nie sieci i systemy informatyczne***, skutecznego przeciwdziałania takim zagrożeniom i ich ograniczania***. Uwzględniając aktualny stan wiedzy i technologii, środki te zapewniają poziom bezpieczeństwa stosowny ***i proporcjonalny*** do istniejącego zagrożenia. W szczególności należy podjąć środki zapobiegające incydentom 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 ***oraz bezpieczeństwo danych*** opartych na tych sieciach i systemach informatycznych.

Poprawka 43

Wniosek dotyczący dyrektywy

Artykuł 14 – ustęp 2 – litera a (nowa)

Poprawka

a) Producenci oprogramowania komercyjnego są pociągani do odpowiedzialności pomimo zawartych w umowach z użytkownikami klauzul o braku odpowiedzialności, w przypadku wystąpienia poważnego zaniedbania w zakresie bezpieczeństwa i ochrony.

Uzasadnienie

W umowie licencyjnej producenci oprogramowania komercyjnego odżegnują się od wszelkiej odpowiedzialności mogącej wynikać ze słabego systemu zabezpieczeń i złej jakości programowania. Aby zachęcić producentów oprogramowania do inwestowania w środki bezpieczeństwa, niezbędne jest wprowadzenie innej kultury przeciwdziałania zagrożeniom. Może to zostać zrealizowane tylko wtedy, gdy producenci oprogramowania są odpowiedzialni za niedociągnięcia w systemie bezpieczeństwa.

Poprawka 44

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Wymogi zawarte w ust. 1 i 2 stosuje się do wszystkich podmiotów gospodarczych świadczących usługi w obrębie Unii Europejskiej.	3. Wymogi zawarte w ust. 1 i 2 stosuje się do wszystkich podmiotów gospodarczych ***i producentów oprogramowania*** świadczących usługi w obrębie Unii Europejskiej.

Poprawka 45

Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 6

Tekst proponowany przez Komisję	*Poprawka*
6. Z zastrzeżeniem wszelkich aktów delegowanych przyjętych na mocy ust. 5, właściwe organy mogą przyjąć wytyczne, a w razie konieczności wydać instrukcje dotyczące okoliczności, w których organy	***skreślony***

administracji publicznej i podmioty gospodarcze są zobowiązane do zgłaszania incydentów.

Poprawka 46

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Państwa członkowskie zapewniają właściwym organom ***wszelkie*** uprawnienia niezbędne do badania przypadków niewypełniania przez organy administracji publicznej lub podmioty gospodarcze zobowiązań ciążących na nich na mocy art. 14 oraz ich wpływu na bezpieczeństwo sieci i systemów informatycznych.	1. Państwa członkowskie zapewniają właściwym organom uprawnienia niezbędne do badania przypadków niewypełniania przez organy administracji publicznej lub podmioty gospodarcze zobowiązań ciążących na nich na mocy art. 14 oraz ich wpływu na bezpieczeństwo sieci i systemów informatycznych.

Poprawka 47

Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. W przypadku incydentów prowadzących do naruszeń danych osobowych właściwe organy działają w ścisłej współpracy z organami ochrony danych osobowych.	5. ***Bez uszczerbku dla mającego zastosowanie prawa o ochronie danych oraz w pełnym porozumieniu z odpowiednimi administratorami danych i podmiotami przetwarzającymi dane,*** w przypadku incydentów prowadzących do naruszeń danych osobowych właściwe organy ***i pojedyncze punkty kontaktowe*** działają w ścisłej współpracy z organami ochrony danych osobowych.

Poprawka 48

Wniosek dotyczący dyrektywy
Artykuł 19 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	Artykuł 19a
	Ochrona i przetwarzanie danych osobowych;
	1. Wszelkie przetwarzanie danych osobowych w państwach członkowskich na mocy niniejszej dyrektywy odbywa się zgodnie z dyrektywą 95/46/WE i dyrektywą 2002/58/WE.
	2. Wszelkie przetwarzanie danych osobowych przez Komisję i ENISA na mocy niniejszej dyrektywy odbywa się zgodnie z rozporządzeniem (WE) nr 45/2001.
	3. Wszelkie przetwarzanie danych osobowych przez działające przy Europolu Centrum ds. Walki z Cyberprzestępczością do celów niniejszej dyrektywy odbywa się na mocy decyzji 2009/371/WSiSW.
	4. Przetwarzanie danych osobowych jest uczciwe i zgodne z prawem oraz ściśle ograniczone do minimalnych danych niezbędnych do celów, w których odbywa się ich przetwarzanie. Są one przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez czas nie dłuższy niż jest to konieczne do celów, w których dane osobowe są przetwarzane.
	5. Zgłaszanie incydentów, o którym mowa w art. 14, pozostaje bez uszczerbku dla określonych w art. 4 dyrektywy 2002/58/WE i w rozporządzeniu (UE) nr 611/2013 przepisów i obowiązków dotyczących powiadamiania o przypadkach naruszenia danych osobowych.
	6. Odniesienia do dyrektywy 95/46/WE należy rozumieć jako odniesienia do

	rozporządzenia Parlamentu Europejskiego i Rady o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych i o swobodnym przepływie takich danych (ogólnego rozporządzenia o ochronie danych), po jego wejściu w życie.

Poprawka 49

Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
Komisja dokonuje okresowego przeglądu funkcjonowania niniejszej dyrektywy i składa Parlamentowi Europejskiemu i Radzie sprawozdania na ten temat. Pierwsze sprawozdanie należy przedłożyć nie później niż ***trzy*** lata po dacie transpozycji, o której mowa w art. 21. W tym celu Komisja może zwrócić się do państw członkowskich o bezzwłoczne dostarczenie informacji.	Komisja dokonuje okresowego przeglądu funkcjonowania niniejszej dyrektywy i składa Parlamentowi Europejskiemu i Radzie sprawozdania na ten temat. Pierwsze sprawozdanie należy przedłożyć nie później niż ***dwa*** lata po dacie transpozycji, o której mowa w art. 21. W tym celu Komisja może zwrócić się do państw członkowskich o bezzwłoczne dostarczenie informacji.

Poprawka 50

Wniosek dotyczący dyrektywy
Artykuł 1 – ustęp 1 – punkt 1 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) CERT wdraża środki mające na celu zapewnienie poufności, integralności, dostępności i wiarygodności otrzymywanych i przetwarzanych informacji**,** oraz zarządza tymi środkami.	b) CERT wdraża środki mające na celu zapewnienie poufności, integralności, dostępności i wiarygodności otrzymywanych i przetwarzanych informacji oraz zarządza tymi środkami**,** ***a także zapewnia ochronę danych***.

Poprawka 51

Wniosek dotyczący dyrektywy
Załącznik 2 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
Wykaz podmiotów gospodarczych	Wykaz podmiotów gospodarczych**,**
o których mowa w art. 3 ust. 8 lit. a):	o których mowa w art. 3 ust. 8 lit. a):
1. platformy handlu elektronicznego	1. platformy handlu elektronicznego
2. internetowe portale płatnicze	2. internetowe portale płatnicze
3. portale społecznościowe	
4. wyszukiwarki	***3***. wyszukiwarki
5. usługi chmur obliczeniowych	***4.*** usługi chmur obliczeniowych ***polegające na przechowywaniu wrażliwych danych Unii Europejskiej na temat infrastruktury krytycznej***
6. sklepy z aplikacjami	

Poprawka 52

Wniosek dotyczący dyrektywy
Artykuł 2 – ustęp 2 – punkt 5 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	5a. łańcuch dostaw żywności

PROCEDURA

Tytuł	Wspólny wysoki poziom bezpieczeństwa sieci i informacji w obrębie Unii			
Odsyłacze	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)			
Komisja przedmiotowo właściwa Data ogłoszenia na posiedzeniu	IMCO 15.4.2013			
Opinia wydana przez Data ogłoszenia na posiedzeniu	LIBE 15.4.2013			
Procedura obejmująca zaangażowane komisje - data ogłoszenia na posiedzeniu	12.9.2013			
Sprawozdawca(czyni) komisji opiniodawczej Data powołania	Carl Schlyter 7.3.2013			
Rozpatrzenie w komisji	25.4.2013	18.9.2013	4.11.2013	13.1.2014
Data przyjęcia	13.1.2014			
Wynik głosowania końcowego	+: –: 0:	36 6 0		
Posłowie obecni podczas głosowania końcowego	Jan Philipp Albrecht, Roberta Angelilli, Edit Bauer, Rita Borsellino, Arkadiusz Tomasz Bratkowski, Philip Claeys, Frank Engel, Cornelia Ernst, Tanja Fajon, Monika Flašíková Beňová, Kinga Gál, Kinga Göncz, Salvatore Iacolino, Sophia in ‘t Veld, Timothy Kirkhope, Juan Fernando López Aguilar, Baroness Sarah Ludford, Monica Luisa Macovei, Svetoslav Hristov Malinov, Véronique Mathieu Houillon, Anthea McIntyre, Nuno Melo, Roberta Metsola, Claude Moraes, Jacek Protasiewicz, Carmen Romero López, Birgit Sippel, Csaba Sógor, Renate Sommer, Axel Voss, Renate Weber, Josef Weidenholzer, Cecilia Wikström, Tatjana Ždanoka, Auke Zijlstra			
Zastępca(y) obecny(i) podczas głosowania końcowego	Monika Hohlmeier, Jean Lambert, Ulrike Lunacek, Jan Mulder, Carl Schlyter, Marco Scurria			
Zastępca(y) (art. 187 ust. 2) obecny(i) podczas głosowania końcowego	Katarína Neveďalová			

06.12.2013

OPINIA KOMISJI SPRAW ZAGRANICZNYCH

dla Komisji Rynku Wewnętrznego i Ochrony Konsumentów

w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Sprawozdawczyni komisji opiniodawczej: Ana Gomes

POPRAWKI

Komisja Spraw Zagranicznych zwraca się do Komisji Rynku Wewnętrznego i Ochrony Konsumentów, jako do komisji przedmiotowo właściwej, o naniesienie w swoim sprawozdaniu następujących poprawek:

Poprawka 1

Wniosek dotyczący dyrektywy
Motyw 1

Tekst proponowany przez Komisję	*Poprawka*
(1) Sieci oraz systemy i usługi informatyczne pełnią w społeczeństwie istotną rolę. Ich niezawodność i bezpieczeństwo mają zasadnicze znaczenie dla działalności gospodarczej i dobrobytu społeczeństwa, a w szczególności dla funkcjonowania rynku wewnętrznego.	(1) Sieci oraz systemy i usługi informatyczne pełnią w społeczeństwie istotną rolę. Ich niezawodność i bezpieczeństwo mają zasadnicze znaczenie dla działalności gospodarczej i dobrobytu społeczeństwa, a w szczególności dla funkcjonowania rynku wewnętrznego***, a także dla bezpieczeństwa zewnętrznego w UE***.

Poprawka 2

Wniosek dotyczący dyrektywy
Motyw 2

Tekst proponowany przez Komisję	*Poprawka*
(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.	(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***, a w konsekwencji stanowić zagrożenie dla dobrobytu obywateli UE oraz zdolności państw członkowskich UE do zapewnienia własnej ochrony oraz bezpieczeństwa infrastruktury krytycznej***.

Poprawka 3

Wniosek dotyczący dyrektywy
Motyw 2 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(2a) Klauzula solidarności wprowadzona na mocy art. 222 TFUE stanowi właściwe ramy wsparcia i wspólnych działań państw członkowskich UE w razie ataku terrorystycznego lub działalności przestępczej stanowiących zagrożenie bezpieczeństwa sieci i informacji. Również klauzula wzajemnej obrony ustanowiona w art. 42 ust. 7 TUE stanowi ramy działań UE w przypadku zbrojnej agresji na jedno z państw członkowskich, która zaszkodziłaby bezpieczeństwu sieci i informacji. We właściwych przypadkach art. 222 TFUE i art. 42 ust. 7 TUE powinny być zastosowane na zasadzie komplementarności.

Poprawka 4

Wniosek dotyczący dyrektywy
Motyw 2 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(2a) Wiele incydentów cybernetycznych wynika z braku odporności i solidności publicznej i prywatnej infrastruktury sieciowej, słabo chronionych lub zabezpieczonych baz danych i innych braków krytycznej infrastruktury i informacji; mając na uwadze, że jedynie nieliczne państwa członkowskie uważają ochronę systemów informacyjnych i związanych z nimi danych za element spoczywającego na nich obowiązku należytej staranności, co uzasadnia brak inwestycji w nowoczesną technologię bezpieczeństwa, szkolenie i opracowanie odpowiednich wytycznych.

Poprawka 5

Wniosek dotyczący dyrektywy
Motyw 3

Tekst proponowany przez Komisję	*Poprawka*
(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	(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.	rynku wewnętrznego***, a także dla bezpieczeństwa wewnętrznego i zewnętrznego UE. Należy zatem należycie podkreślić potrzebę poprawy bezpieczeństwa sieci i informacji w unijnej strategii bezpieczeństwa wewnętrznego oraz w europejskiej strategii bezpieczeństwa, w szczególności z myślą o przyszłym przeglądzie tych dokumentów.***

Poprawka 6

Wniosek dotyczący dyrektywy
Motyw 3 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(3a) Uświadamianie i kształcenie użytkowników technologii informacyjnych i komunikacyjnych w zakresie najlepszych wzorców zabezpieczania danych osobowych, a także trwałego utrzymywania usług komunikacyjnych powinno stanowić podstawę każdej kompleksowej strategii bezpieczeństwa cybernetycznego.

Poprawka 7

Wniosek dotyczący dyrektywy
Motyw 4 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(4a) Współpraca i koordynacja między właściwymi organami unijnymi a wysokim przedstawicielem/wiceprzewodniczącym Komisji – odpowiedzialnymi za wspólną politykę zagraniczną i bezpieczeństwa oraz wspólną politykę bezpieczeństwa i obrony – i koordynatorem UE ds. zwalczania terroryzmu powinny zostać zagwarantowane we wszystkich

przypadkach, w których może zaistnieć zagrożenie z zewnątrz i o charakterze terrorystycznym.

Poprawka 8

Wniosek dotyczący dyrektywy
Motyw 4 b (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(4b) W oparciu o zasadę zaufania, solidarności i współpracy należy poprawić przekazywanie między państwami członkowskimi oraz między państwami członkowskimi a właściwymi organami UE informacji poufnych i pozyskanych przez wywiad. Wszelki plan działania służący poprawie bezpieczeństwa sieci i systemu powinien zatem w pełni wykorzystać istniejące już w UE struktury, takie jak SitCen i IntCen, oraz zapewnić koordynację wszystkich struktur właściwych dla bezpieczeństwa informacji poufnych, istotnych dla bezpieczeństwa wewnętrznego i zewnętrznego UE.

Poprawka 9

Wniosek dotyczący dyrektywy
Motyw 4 c (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(4c) Współpraca i dzielenie się informacjami na szczeblu światowym z właściwymi partnerami międzynarodowymi jest kluczowe dla skuteczności strategii bezpieczeństwa cybernetycznego oraz przekonujących działań służących zwiększeniu bezpieczeństwa sieci i informacji w UE, w obliczu międzynarodowego charakteru zagrożenia.

Poprawka 10

Wniosek dotyczący dyrektywy
Motyw 8 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(8a) Środki bezpieczeństwa nie mogą naruszać podstawowych praw przysługujących UE i jej państwom członkowskim zgodnie z art. 2, 6 i 21 TFUE, takich jak wolność słowa, ochrona danych i prywatność; mając na uwadze, że prawo do prywatności i ochrony danych jest zapisane w Karcie praw podstawowych UE i w art. 16 TFUE.

Poprawka 11

Wniosek dotyczący dyrektywy
Motyw 11 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(11a) Wszystkie państwa członkowskie skupiają się w krajowych strategiach cyberbezpieczeństwa na ochronie systemów informacyjnych i związanych z nimi danych oraz uznają ochronę tej krytycznej infrastruktury za część spoczywającego na każdym z ich obowiązku należytej staranności. Wszystkie państwa członkowskie przyjmują i wdrażają strategie, wytyczne i instrumenty, które zapewniają rozsądne poziomy ochrony przed rozsądnie identyfikowalnymi poziomami zagrożeń, przy kosztach i obciążeniach związanych z ochroną proporcjonalnych do prawdopodobnej szkody dla zainteresowanych stron. Wszystkie państwa członkowskie podejmują również odpowiednie działania w celu zobowiązania osób prawnych

	pozostających w ich właściwości sądowej do ochrony danych osobowych pozostających w ich dyspozycji.

Poprawka 12

Wniosek dotyczący dyrektywy
Motyw 16

Tekst proponowany przez Komisję	*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.	(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. ***Dane osobowe publikowane na takiej stronie internetowej powinny być ograniczone do niezbędnego minimum i pozwalać na zachowanie anonimowości w największym możliwym stopniu.***

Poprawka 13

Wniosek dotyczący dyrektywy
Motyw 30 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(30a) Niniejsza dyrektywa pozostaje bez uszczerbku dla unijnego dorobku prawnego dotyczącego ochrony danych. Dane osobowe wykorzystywane zgodnie z przepisami niniejszej dyrektywy powinny ograniczać się do minimum absolutnie niezbędnych danych osobowych i być przekazywane wyłącznie absolutnie niezbędnym podmiotom oraz pozwalać na zachowanie anonimowości w największym możliwym stopniu lub nawet zachowanie całkowitej anonimowości.

Poprawka 14

Wniosek dotyczący dyrektywy
Motyw 32 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(32a) Niniejsza dyrektywa w sprawie bezpieczeństwa sieci i informacji nie jest przeszkodą dla przyjęcia niezbędnego prawodawstwa UE dotyczącego ochrony danych.

Poprawka 15

Wniosek dotyczący dyrektywy
Motyw 34 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(34a) Istnieje potrzeba regulacji na szczeblu unijnym kwestii sprzedaży, dostawy, transferu lub wywozu do krajów trzecich sprzętu lub oprogramowania, którego pierwotnym przeznaczeniem jest monitorowanie lub przechwytywanie połączeń internetowych i telefonicznych w sieciach mobilnych lub stałych, oraz przepisów dotyczących pomocy w instalowaniu, działaniu czy aktualizowaniu takiego sprzętu lub oprogramowania. Komisja musi, najszybciej jak to możliwe, przygotować ustawodawstwo uniemożliwiające spółkom europejskim eksport takich produktów podwójnego zastosowania do miejsc, gdzie panują niedemokratyczne, autorytarne i represyjne reżimy.

Poprawka 16

Wniosek dotyczący dyrektywy
Artykuł 1 – ustęp 2 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) ustanawia mechanizm współpracy między państwami członkowskimi w celu zapewnienia jednolitego stosowania niniejszej dyrektywy w obrębie Unii oraz, w razie konieczności, w celu zapewnienia skoordynowanego ***i*** sprawnego postępowania w przypadku wystąpienia zagrożeń i incydentów dotyczących sieci i systemów informatycznych oraz reagowania na nie;	b) ustanawia mechanizm współpracy między państwami członkowskimi w celu zapewnienia jednolitego stosowania niniejszej dyrektywy w obrębie Unii oraz, w razie konieczności, w celu zapewnienia skoordynowanego***,*** sprawnego ***i skutecznego*** postępowania w przypadku wystąpienia zagrożeń i incydentów dotyczących sieci i systemów informatycznych oraz reagowania na nie;

Poprawka 17

Wniosek dotyczący dyrektywy
Artykuł 3 – ustęp 1 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) wszelkie ***urządzenia lub*** grupy połączonych lub powiązanych urządzeń, z których jedno lub więcej, zgodnie z oprogramowaniem, dokonuje automatycznego przetwarzania danych komputerowych, jak również	b) wszelkie grupy połączonych lub powiązanych urządzeń, z których jedno lub więcej, zgodnie z oprogramowaniem, dokonuje automatycznego przetwarzania danych komputerowych, jak również

Poprawka 18

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

Tekst proponowany przez Komisję	*Poprawka*
	a) „odporność na zagrożenia cybernetyczne" oznacza zdolność sieci i systemów informacyjnych do oparcia się zagrożeniu i powrotu do pełnej zdolności operacyjnej po incydentach, w tym – między innymi – takich jak niesprawność

	techniczna, awarie zasilania lub incydenty dotyczące bezpieczeństwa;

Poprawka 19

Wniosek dotyczący dyrektywy
Artykuł 3 – ustęp 8 – litera b

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

Poprawka 20

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

Tekst proponowany przez Komisję	*Poprawka*
	ba) dostawców urządzeń, sieci i systemów informatycznych, o których mowa w ust. 1, lub ich komponentów, które są istotne dla zapewnienia wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji.

Poprawka 21

Wniosek dotyczący dyrektywy
Artykuł 6 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Każde państwo członkowskie wyznacza właściwy organ krajowy ds. bezpieczeństwa sieci i systemów	1. Każde państwo członkowskie wyznacza właściwy ***cywilny*** organ krajowy ds. bezpieczeństwa sieci i systemów

informatycznych („właściwy organ”).	informatycznych („właściwy organ”).

Poprawka 22

Wniosek dotyczący dyrektywy
Artykuł 7 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Każde państwo członkowskie ustanawia zespół reagowania na incydenty komputerowe (zwany dalej „CERT”), odpowiedzialny za postępowanie w przypadku wystąpienia incydentów i zagrożeń według jasno określonej procedury, która jest zgodna z wymogami określonymi w załączniku I pkt 1. CERT może zostać ustanowiony w ramach właściwego organu.	1. Każde państwo członkowskie ustanawia ***przynajmniej jeden*** zespół reagowania na incydenty komputerowe (zwany dalej „CERT”), odpowiedzialny za postępowanie w przypadku wystąpienia incydentów i zagrożeń według jasno określonej procedury, która jest zgodna z wymogami określonymi w załączniku I pkt 1. CERT może zostać ustanowiony w ramach właściwego organu.

Poprawka 23

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

Tekst proponowany przez Komisję	*Poprawka*
	fa) we właściwych przypadkach, mając na uwadze rodzaj ryzyka lub zagrożenia, koordynator UE ds. zwalczania terroryzmu powinien zostać poinformowany za pośrednictwem sprawozdania i może zostać poproszony o pomoc w postaci analizy prac przygotowawczych i działań sieci współpracy;

Poprawka 24

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.

Poprawka 25

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.	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***, zgodnie z przepisami ogólnego rozporządzenia o ochronie danych***.

Poprawka 26

Wniosek dotyczący dyrektywy
Artykuł 13 – ustęp -1 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	-1a. Wysoki przedstawiciel / wiceprzewodniczący uwzględnia w działaniach zewnętrznych UE (zwłaszcza w zakresie stosunków z państwami trzecimi) aspekty bezpieczeństwa cybernetycznego. Celem jest wzmożona wymiana doświadczeń i współpraca w dziedzinie bezpieczeństwa

cybernetycznego.

Poprawka 27

Wniosek dotyczący dyrektywy
Artykuł 13 – ustęp -1 b (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	-1b. Rada i Komisja w ramach stosunków z państwami trzecimi i umów o współpracę z tymi państwami, zwłaszcza w dziedzinie technologii, powinny kłaść nacisk na przestrzeganie minimalnych norm bezpieczeństwa systemów informatycznych.

Poprawka 28

Wniosek dotyczący dyrektywy
Artykuł 20 – tytuł

Tekst proponowany przez Komisję	*Poprawka*
Przegląd	***Sprawozdawczość i*** przegląd

Poprawka 29

Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp -1 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	-1a. Komisja przedstawia roczne sprawozdanie na temat incydentów i środków wobec nich zastosowanych na mocy niniejszej dyrektywy Parlamentu Europejskiego i Rady.

Poprawka 30

Wniosek dotyczący dyrektywy
Załącznik 1 – ustęp 1 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) CERT wdraża środki mające na celu zapewnienie poufności, integralności, dostępności i wiarygodności otrzymywanych i przetwarzanych informacji, oraz zarządza tymi środkami.	b) CERT wdraża środki mające na celu zapewnienie poufności, integralności, dostępności i wiarygodności otrzymywanych i przetwarzanych informacji, oraz zarządza tymi środkami***, zgodnie z wymogami dotyczącymi ochrony danych***.

Poprawka 31

Wniosek dotyczący dyrektywy
ZAŁĄCZNIK II – drugi podtytuł (o którym mowa w art. 3 ust. 8 lit. b) – ustęp 5 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	5a. Bezpieczeństwo i obrona: podmioty gospodarcze prowadzące działalność i świadczące usługi, o których mowa w dyrektywie 2009/81/WE, w szczególności w jej art. 46

PROCEDURA

Tytuł	Wspólny wysoki poziom bezpieczeństwa sieci i informacji w obrębie Unii
Odsyłacze	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)
Komisja przedmiotowo właściwa Data ogłoszenia na posiedzeniu	IMCO 15.4.2013
Opinia wydana przez Data ogłoszenia na posiedzeniu	AFET 15.4.2013
Sprawozdawca(czyni) komisji opiniodawczej Data powołania	Ana Gomes 19.2.2013
Rozpatrzenie w komisji	18.9.2013
Data przyjęcia	5.12.2013
Wynik głosowania końcowego	+: 31 –: 3 0: 8
Posłowie obecni podczas głosowania końcowego	Elmar Brok, Jerzy Buzek, Mark Demesmaeker, Marietta Giannakou, Ana Gomes, Andrzej Grzyb, Anna Ibrisagic, Jelko Kacin, Tunne Kelam, Nicole Kiil-Nielsen, Andrey Kovatchev, Eduard Kukan, Marusya Lyubcheva, Annemie Neyts-Uyttebroeck, Norica Nicolai, Raimon Obiols, Kristiina Ojuland, Ria Oomen-Ruijten, Ioan Mircea Paşcu, Alojz Peterle, Mirosław Piotrowski, Bernd Posselt, Hans-Gert Pöttering, Cristian Dan Preda, Libor Rouček, Tokia Saïfi, José Ignacio Salafranca Sánchez-Neyra, György Schöpflin, Werner Schulz, Marek Siwiec, Charles Tannock, Geoffrey Van Orden, Nikola Vuljanić, Boris Zala
Zastępca(y) obecny(i) podczas głosowania końcowego	Marije Cornelissen, Barbara Lochbihler, Doris Pack, Marietje Schaake, Indrek Tarand, Ivo Vajgl, Paweł Zalewski
Zastępca(y) (art. 187 ust. 2) obecny(i) podczas głosowania końcowego	Hiltrud Breyer

PROCEDURA

Tytuł	Wspólny wysoki poziom bezpieczeństwa sieci i informacji w obrębie Unii			
Odsyłacze	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)			
Data przedstawienia w PE	5.2.2013			
Komisja przedmiotowo właściwa Data ogłoszenia na posiedzeniu	IMCO 15.4.2013			
Komisja(e) wyznaczona(e) do wydania opinii Data ogłoszenia na posiedzeniu	AFET 15.4.2013	INTA 15.4.2013	BUDG 15.4.2013	ECON 15.4.2013
	ENVI 15.4.2013	ITRE 15.4.2013	TRAN 15.4.2013	JURI 15.4.2013
	LIBE 15.4.2013			
Opinia niewydana Data decyzji	INTA 20.3.2013	BUDG 21.2.2013	ECON 18.6.2013	ENVI 19.2.2013
	TRAN 18.3.2013	JURI 20.2.2013		
Procedura obejmująca zaangażowane komisje Data ogłoszenia na posiedzeniu	ITRE 12.9.2013	LIBE 12.9.2013		
Sprawozdawca(y) Data powołania	Andreas Schwab 20.3.2013			
Rozpatrzenie w komisji	25.4.2013	18.6.2013	5.9.2013	4.11.2013
	9.1.2014			
Data przyjęcia	23.1.2014			
Wynik głosowania końcowego	+: –: 0:	33 1 1		
Posłowie obecni podczas głosowania końcowego	Claudette Abela Baldacchino, Pablo Arias Echeverría, Adam Bielan, Preslav Borissov, Sergio Gaetano Cofferati, Lara Comi, Anna Maria Corazza Bildt, Christian Engström, Vicente Miguel Garcés Ramón, Evelyne Gebhardt, Małgorzata Handzlik, Eduard-Raul Hellvig, Sandra Kalniete, Edvard Kožušník, Toine Manders, Hans-Peter Mayer, Franz Obermayr, Sirpa Pietikäinen, Zuzana Roithová, Heide Rühle, Andreas Schwab, Róża Gräfin von Thun und Hohenstein, Bernadette Vergnaud, Barbara Weiler			
Zastępca(y) obecny(i) podczas głosowania końcowego	Regina Bastos, Ashley Fox, María Irigoyen Pérez, Morten Løkkegaard, Tadeusz Ross, Marc Tarabella, Patricia van der Kammen, Sabine Verheyen, Josef Weidenholzer			
Zastępca(y) (art. 187 ust. 2) obecny(i)	Vital Moreira, Oreste Rossi			

podczas głosowania końcowego	
Data złożenia	12.2.2014