KOMISJA
EUROPEJSKA

Bruksela, dnia 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

Wniosek

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

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

{SWD(2013) 31 final}
{SWD(2013) 32 final}

UZASADNIENIE

Celem proponowanej dyrektywy jest zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji (ang. *network and information security*, NIS). Oznacza to zwiększenie bezpieczeństwa internetu oraz prywatnych sieci i systemów informatycznych stanowiących podstawę funkcjonowania naszych społeczeństw i gospodarek. Cel ten zostanie osiągnięty poprzez nałożenie na państwa członkowskie obowiązku zwiększenia gotowości i ulepszenia wzajemnej współpracy oraz poprzez nałożenie na operatorów infrastruktury krytycznej, w takich dziedzinach jak energetyka, transport i kluczowe usługi społeczeństwa informacyjnego (platformy handlu elektronicznego, serwisy społecznościowe itd.), jak również na organy administracji publicznej, obowiązku podjęcia odpowiednich działań mających na celu przeciwdziałanie zagrożeniom bezpieczeństwa oraz obowiązku zgłaszania poważnych incydentów właściwym organom krajowym.

Wniosek ten zostaje przedstawiony łącznie ze wspólnym komunikatem Komisji i Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa w sprawie europejskiej strategii bezpieczeństwa cybernetycznego. Celem strategii jest zapewnienie bezpiecznego i wiarygodnego środowiska cyfrowego, a także jednoczesne propagowanie i ochrona praw podstawowych i innych podstawowych wartości UE. Przedstawienie niniejszego wniosku stanowi realizację głównego działania przewidzianego w strategii. Dalsze działania w ramach strategii w tej dziedzinie koncentrują się na szerzeniu wiedzy, rozwijaniu rynku wewnętrznego produktów i usług związanych z bezpieczeństwem cybernetycznym oraz wspieraniu inwestycji w badania i rozwój. Działania te zostaną uzupełnione innymi działaniami mającymi na celu intensyfikację walki z cyberprzestępczością oraz opracowanie międzynarodowej polityki w zakresie bezpieczeństwa cybernetycznego dla UE.

1.1. Podstawa i cele wniosku

Bezpieczeństwo sieci i informacji ma coraz większe znaczenie dla naszej gospodarki i dla całego społeczeństwa. Zapewnienie bezpieczeństwa sieci i informacji jest również ważnym warunkiem utworzenia wiarygodnego środowiska dla światowego handlu usługami. Systemy informatyczne są jednak narażone na incydenty zagrażające bezpieczeństwu, takie jak ludzkie błędy, zjawiska naturalne, awarie techniczne lub celowe ataki. Incydenty te mają miejsce coraz częściej oraz stają się coraz bardziej poważne i złożone. Z przeprowadzonych przez Komisję internetowych konsultacji społecznych w sprawie poprawy bezpieczeństwa sieci i informacji w UE[1] wynika, że w ubiegłym roku 57 % respondentów doświadczyło incydentów w zakresie bezpieczeństwa sieci i informacji, które miały poważny wpływ na ich działalność. Brak bezpieczeństwa sieci i informacji może zagrażać kluczowym usługom uzależnionym od integralności sieci i systemów informatycznych. Może to uniemożliwić funkcjonowanie przedsiębiorstw, przynieść znaczne straty finansowe dla gospodarki UE i negatywnie wpłynąć na poziom dobrobytu społecznego.

Ponadto cyfrowe systemy informatyczne – w szczególności internet – które służą do komunikacji ponad granicami, łączą ze sobą państwa członkowskie i odgrywają istotną rolę w ułatwianiu transgranicznego przepływu towarów, usług i osób. Poważne zakłócenia tych systemów w jednym państwie członkowskim mogą mieć wpływ na inne państwa członkowskie i na całą UE. Odporność i stabilność sieci i systemów informatycznych mają zatem zasadnicze znaczenie dla zakończenia tworzenia jednolitego rynku cyfrowego i dla sprawnego funkcjonowania rynku wewnętrznego. Prawdopodobieństwo i częstotliwość

[1] Internetowe konsultacje społeczne w sprawie poprawy bezpieczeństwa sieci i informacji w UE trwały od 23 lipca do 15 października 2012 r.

występowania incydentów i niemożność zapewnienia skutecznej ochrony zmniejszają również społeczne zaufanie do sieci i usług informatycznych. Przykładowo, w 2012 r. badanie Eurobarometru na temat bezpieczeństwa cybernetycznego wykazało, że 38 % internautów ma wątpliwości co do bezpieczeństwa płatności internetowych i zmieniło swoje zachowania ze względu na kwestie bezpieczeństwa: 18 % jest mniej przekonanych do robienia zakupów przez internet, a 15 % jest mniej przekonanych do korzystania z internetowych usług bankowych[2].

Obecny stan rzeczy w UE, który odzwierciedla przyjęte do tej pory czysto dobrowolne podejście, nie zapewnia wystarczającej ochrony przed incydentami w zakresie bezpieczeństwa sieci i informacji oraz przed zagrożeniami w obrębie całej UE. Istniejące zdolności i mechanizmy w zakresie bezpieczeństwa sieci i informacji nie są wystarczające, aby odpowiednio reagować na szybko zmieniające się zagrożenia i zapewnić wspólny wysoki poziom ochrony we wszystkich państwach członkowskich.

Pomimo podjętych inicjatyw państwa członkowskie mają bardzo różne poziomy zdolności i gotowości, co prowadzi do fragmentacji podejścia w całej UE. Ze względu na fakt, iż systemy i sieci są wzajemnie połączone, ogólny poziom bezpieczeństwa sieci i informacji w UE jest obniżony przez państwa członkowskie nieposiadające odpowiedniego poziomu ochrony. Sytuacja ta utrudnia również budowanie zaufania między partnerami, co jest warunkiem niezbędnym do współpracy i wymiany informacji. W rezultacie współpraca ma miejsce jedynie w przypadku będących w mniejszości państw członkowskich posiadających wysoki poziom zdolności.

W związku z tym na poziomie UE nie ma obecnie skutecznych mechanizmów współpracy i współdziałania ani mechanizmów, za pomocą których państwa członkowskie mogłyby wymieniać między sobą informacje dotyczące incydentów oraz zagrożeń w zakresie bezpieczeństwa sieci i informacji. Skutkiem takiego stanu rzeczy mogą być nieskoordynowane interwencje regulacyjne, niespójne strategie i rozbieżne normy, a w efekcie niewystarczająca ochrona bezpieczeństwa sieci i informacji w całej UE. Mogą również powstać bariery na rynku wewnętrznym wynikające z faktu, iż przedsiębiorstwa działające w więcej niż jednym państwie członkowskim będą narażone na koszty związane z koniecznością dostosowania się do różnych przepisów.

Ponadto podmioty zarządzające infrastrukturą krytyczną lub świadczące usługi niezbędne do funkcjonowania naszych społeczeństw nie są zobowiązane do przyjęcia środków przeciwdziałania zagrożeniom ani do wymiany informacji z właściwymi organami. Tak więc z jednej strony brakuje skutecznych bodźców, które zmusiłyby przedsiębiorstwa do odpowiedniego przeciwdziałania zagrożeniom, łącznie z przeprowadzaniem oceny zagrożeń i podejmowaniem odpowiednich kroków w celu zapewnienia bezpieczeństwa sieci i informacji. Z drugiej strony informacje o znacznej części incydentów nie docierają do właściwych organów i incydenty takie pozostają niezauważone. Informacje dotyczące incydentów mają jednak zasadnicze znaczenie dla władz publicznych, ponieważ umożliwiają im reagowanie, podejmowanie odpowiednich środków łagodzących oraz ustalanie odpowiednich priorytetów strategicznych w zakresie bezpieczeństwa sieci i informacji.

Zgodnie z obecnymi ramami regulacyjnymi jedynie przedsiębiorstwa telekomunikacyjne są zobowiązane do przyjmowania środków przeciwdziałania zagrożeniom i zgłaszania poważnych incydentów w zakresie bezpieczeństwa sieci i informacji. Jednakże działalność w wielu innych branżach jest również uzależniona od technologii informacyjno-komunikacyjnych (ICT), a zatem także w tych przypadkach bezpieczeństwo sieci i informacji powinno stanowić istotną kwestię. Niektórzy konkretni dostawcy infrastruktury i usług są

[2] Eurobarometr 390/2012.

szczególnie narażeni ze względu na wysoki stopień uzależnienia ich działalności od prawidłowego funkcjonowania sieci i systemów informatycznych. Branże te odgrywają zasadniczą rolę w zapewnianiu podstawowych usług wsparcia dla naszej gospodarki i społeczeństwa, a bezpieczeństwo ich systemów ma szczególne znaczenie dla funkcjonowania rynku wewnętrznego. Sektory te obejmują bankowość, giełdy, wytwarzanie, przesyłanie i dystrybucję energii, transport (lotniczy, kolejowy, morski), opiekę zdrowotną, usługi internetowe i administrację publiczną.

W związku z tym konieczne jest wprowadzenie gruntownych zmian w zakresie bezpieczeństwa sieci i informacji w UE. Konieczne jest wprowadzenie wymogów prawnych w celu zapewnienia równych warunków działania i usunięcia istniejących luk prawnych. Aby rozwiązać te problemy i zwiększyć poziom bezpieczeństwa sieci i informacji w Unii Europejskiej, w proponowanej dyrektywie wyznaczono opisane niżej cele.

Po pierwsze, wniosek zobowiązuje wszystkie państwa członkowskie do zagwarantowania minimalnego poziomu krajowych zdolności poprzez ustanowienie właściwych organów ds. bezpieczeństwa sieci i informacji, powołanie zespołów reagowania na incydenty komputerowe (CERT) oraz przyjęcie krajowych strategii i planów współpracy w zakresie bezpieczeństwa sieci i informacji.

Po drugie, właściwe organy krajowe powinny współpracować w ramach sieci umożliwiającej bezpieczną i skuteczną koordynację, w tym skoordynowaną wymianę informacji, jak również wykrywanie i reagowanie na poziomie UE. Poprzez tę sieć państwa członkowskie powinny wymieniać się informacjami i współpracować ze sobą w celu zwalczania zagrożeń i incydentów w zakresie bezpieczeństwa sieci i informacji na podstawie europejskiego planu współpracy w tej dziedzinie.

Po trzecie, opierając się na modelu, jakim jest dyrektywa ramowa w sprawie łączności elektronicznej, wniosek ma na celu zapewnienie rozwoju kultury wspierającej przeciwdziałanie zagrożeniom oraz wymiany informacji między sektorem prywatnym i publicznym. Przedsiębiorstwa w określonych krytycznych sektorach wymienionych powyżej oraz administracje publiczne będą zobowiązane do dokonania oceny zagrożeń, na jakie są narażone, oraz do przyjęcia odpowiednich i proporcjonalnych środków mających na celu zapewnienie bezpieczeństwa sieci i informacji. Podmioty te będą zobowiązane do zgłaszania właściwym organom wszelkich incydentów poważnie zagrażających ich sieciom i systemom informatycznym oraz mogących znacząco zakłócić ciągłość krytycznych usług i dostaw towarów.

1.2. Kontekst ogólny

Już w komunikacie z 2001 r. pt. „Bezpieczeństwo sieci i informacji: Propozycje na rzecz europejskiego podejścia”[3] Komisja podkreśliła coraz większe znaczenie bezpieczeństwa sieci i informacji. Z kolei w 2006 r. przyjęto strategię na rzecz bezpiecznego społeczeństwa informacyjnego[4], której celem był rozwój kultury bezpieczeństwa sieci i informacji w Europie. Główne elementy tej strategii zostały przyjęte w rezolucji Rady[5].

Następnie, w dniu 30 marca 2009 r., Komisja przyjęła komunikat w sprawie ochrony krytycznej infrastruktury informatycznej (CIIP)[6], który dotyczył zapewnienia ochrony Europy przed zakłóceniami cybernetycznymi poprzez zwiększenie bezpieczeństwa. Komunikat ten doprowadził do opracowania planu działania, którego celem było wsparcie działań państw

---

3 COM(2001) 298.
4 COM(2006) 251 http://eur-lex.europa.eu/LexUriServ/site/pl/com/2006/com2006_0251pl01.pdf.
5 2007/068/01.
6 COM(2009) 149.

członkowskich w zakresie zapobiegania zakłóceniom cybernetycznym i reagowania na nie. Plan działania został zatwierdzony w konkluzjach prezydencji z konferencji ministerialnej w sprawie ochrony krytycznej infrastruktury informatycznej, która odbyła się w Tallinie w 2009 r. W dniu 18 grudnia 2009 r. Rada przyjęła rezolucję w sprawie wspólnego europejskiego podejścia do bezpieczeństwa sieci i informacji[7].

W Europejskiej agendzie cyfrowej[8], przyjętej w maju 2010 r., oraz w powiązanych z nią konkluzjach Rady[9], podkreślono zgodę co do tego, że zaufanie i bezpieczeństwo są istotnymi warunkami niezbędnymi do umożliwienia rozpowszechnienia ICT, a przez to do osiągnięcia celów związanych z inteligentnym wzrostem gospodarczym, zapisanych w strategii „Europa 2020"[10]. W rozdziale Europejskiej agendy cyfrowej dotyczącym zaufania i bezpieczeństwa podkreślono, że w celu zapewnienia bezpieczeństwa i odporności infrastruktury ICT konieczne jest podjęcie przez wszystkie zainteresowane strony wspólnych, kompleksowych działań, które koncentrować się będą na zapobieganiu, gotowości i uświadamianiu, a także na stworzeniu skutecznych i skoordynowanych mechanizmów bezpieczeństwa. W szczególności w ramach głównego działania nr 6 określonego w Europejskiej agendzie cyfrowej apeluje się o wprowadzenie środków ukierunkowanych na prowadzenie na wysokim szczeblu udoskonalonej polityki w zakresie bezpieczeństwa sieci i informacji.

W komunikacie w sprawie ochrony krytycznej infrastruktury informatycznej z marca 2011 r. zatytułowanym „Osiągnięcia i dalsze działania na rzecz globalnego bezpieczeństwa cyberprzestrzeni"[11] Komisja podsumowała wyniki osiągnięte od momentu przyjęcia planu działania na rzecz ochrony krytycznej infrastruktury teleinformatycznej w 2009 r., dochodząc w świetle doświadczeń w realizacji tego planu do wniosku, że stosowanie jedynie rozwiązań krajowych w kwestiach związanych z bezpieczeństwem i odpornością nie jest wystarczające, oraz że Europa powinna kontynuować swoje działania na rzecz wypracowania spójnego podejścia opartego na współpracy w całej UE. W komunikacie w sprawie ochrony krytycznej infrastruktury teleinformatycznej z 2011 r. zapowiedziano szereg działań, a Komisja wezwała państwa członkowskie do utworzenia zdolności w zakresie bezpieczeństwa sieci i informacji oraz do podjęcia współpracy transgranicznej. Mimo iż większość tych działań miała zostać zakończona w 2012 r., nie zostały one jeszcze zrealizowane.

W konkluzjach z dnia 27 maja 2011 r. w sprawie ochrony krytycznej infrastruktury teleinformatycznej Rada Unii Europejskiej zwróciła uwagę na pilną potrzebę zapewnienia odporności systemów i sieci ICT oraz ich zabezpieczenia przed wszelkimi możliwymi zakłóceniami, przypadkowymi bądź umyślnymi, zapewnienia w całej UE wysokiego poziomu gotowości, bezpieczeństwa i odporności oraz modernizacji zdolności technicznych, tak aby umożliwić Europie sprostanie wyzwaniu, jakim jest zapewnienie ochrony sieci i infrastruktury informatycznej, oraz aby stymulować współpracę między państwami członkowskimi poprzez tworzenie mechanizmów współpracy między państwami członkowskimi w przypadku wystąpienia incydentów.

1.3. Obowiązujące przepisy Unii Europejskiej i przepisy międzynarodowe w przedmiotowej dziedzinie

Zgodnie z rozporządzeniem (WE) nr 460/2004 Wspólnota Europejska ustanowiła w 2004 r. Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA)[12], której celem jest

---

7 2009/C 321/01.
8 COM(2010) 245.
9 Konkluzje Rady z dnia 31 maja 2010 r. w sprawie Europejskiej agendy cyfrowej (10130/10).
10 COM(2010) 2020 oraz konkluzje Rady Europejskiej z dnia 25/26 marca 2010 (EUCO 7/10).
11 COM(2011) 163.
12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:PL:HTML

przyczynianie się do rozwoju i zapewnienie wysokiego poziomu kultury bezpieczeństwa sieci i informacji na terenie UE. W dniu 30 września 2010 r. przyjęto wniosek mający na celu unowocześnienie ENISA[13], który jest obecnie przedmiotem obrad w Radzie i Parlamencie Europejskim. W zmienionych ramach regulacyjnych dotyczących łączności elektronicznej[14], obowiązujących od listopada 2009 r., na dostawców usług łączności elektronicznej nałożono obowiązki w zakresie bezpieczeństwa[15]. Obowiązki te miały zostać transponowane do prawa krajowego do maja 2011 r.

Na mocy ram prawnych dotyczących ochrony danych[16] wszystkie podmioty, które są administratorami danych (na przykład banki i szpitale), są zobowiązane do wprowadzenia w życie środków bezpieczeństwa w celu ochrony danych osobowych. Ponadto, zgodnie z wnioskiem Komisji z 2012 r. dotyczącym ogólnego rozporządzenia o ochronie danych[17], administratorzy danych będą zobowiązani do zgłaszania krajowym organom nadzoru przypadków naruszenia przepisów o ochronie danych. Oznacza to, że na przykład naruszenie bezpieczeństwa sieci i informacji mające wpływ na świadczenie danej usługi, lecz niezagrażające bezpieczeństwu danych osobowych (takie jak np. awaria systemów ICT w przedsiębiorstwie energetycznym prowadząca do przerwy w dostawie energii elektrycznej), nie podlegałoby obowiązkowi zgłoszenia.

Na mocy dyrektywy 2008/114 w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, w europejskim programie ochrony infrastruktury krytycznej (EPCIP)[18] przedstawiono ogólne podejście w zakresie ochrony infrastruktury krytycznej w UE. Cele EPCIP są w pełni zgodne z niniejszym wnioskiem, a dyrektywę należy stosować bez uszczerbku dla przepisów dyrektywy 2008/114. EPCIP nie zobowiązuje podmiotów do zgłaszania poważnych naruszeń bezpieczeństwa i nie ustanawia mechanizmów, za pomocą których państwa członkowskie mogłyby współpracować i reagować na incydenty.

Współprawodawcy prowadzą obecnie rozmowy na temat wniosku Komisji dotyczącego dyrektywy w sprawie ataków na systemy informatyczne[19], która ma na celu harmonizację kryminalizacji niektórych rodzajów zachowań. Dotyczy ona jednak tylko kryminalizacji niektórych rodzajów zachowań i nie uwzględnia kwestii zapobiegania zagrożeniom i incydentom w zakresie bezpieczeństwa sieci i informacji, reagowania na takie incydenty oraz łagodzenia ich skutków. Niniejsza dyrektywa powinna mieć zastosowanie bez uszczerbku dla dyrektywy w sprawie ataków na systemy informatyczne.

W dniu 28 marca 2012 r. Komisja przyjęła komunikat w sprawie ustanowienia Europejskiego Centrum ds. Walki z Cyberprzestępczością (EC3)[20]. Centrum to, ustanowione w dniu 11 stycznia 2013 r., stanowi część Europejskiego Urzędu Policji (Europol) i będzie działać jako centralny punkt kontaktowy do spraw zwalczania cyberprzestępczości w UE. Celem EC3 jest gromadzenie dostępnej w Europie wiedzy specjalistycznej na temat cyberprzestępczości potrzebnej do budowania zdolności przez państwa członkowskie, wspieranie państw członkowskich w prowadzeniu dochodzeń dotyczących cyberprzestępczości, a także – w

---

13 COM(2010) 521.

14 Zob. http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

15 Artykuły 13a i 13b dyrektywy ramowej.

16 Dyrektywa 2002/58 z 12 lipca 2002 r.

17 COM(2012) 11.

18 COM(2006) 786 http://eur-lex.europa.eu/LexUriServ/site/pl/com/2006/com2006_0786pl01.pdf.

19 COM(2010) 517 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:PL:PDF.

20 COM(2012) 140 http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:PL:PDF.

ścisłej współpracy z Eurojustem – zapewnienie zbiorowego głosu dla podmiotów prowadzących takie dochodzenia w Europie w ramach organów ścigania i wymiaru sprawiedliwości.

Instytucje, agencje i organy europejskie powołały własne zespoły reagowania na incydenty komputerowe (ang. *Computer Emergency Response Teams*, CERT-UE).

Na poziomie międzynarodowym UE prowadzi działania na rzecz bezpieczeństwa cybernetycznego zarówno w ramach kontaktów dwustronnych, jak i wielostronnych. Podczas szczytu UE-USA w 2010 r.[21] powołano grupę roboczą UE-USA ds. bezpieczeństwa cybernetycznego i cyberprzestępczości. UE działa również aktywnie na innych stosownych forach wielostronnych, takich jak Organizacja Współpracy Gospodarczej i Rozwoju (OECD), Zgromadzenie Ogólne Narodów Zjednoczonych (ZO ONZ), Międzynarodowy Związek Telekomunikacyjny (ITU), Organizacja Bezpieczeństwa i Współpracy w Europie (OBWE), Światowy Szczyt Społeczeństwa Informacyjnego (WSIS) oraz Forum Zarządzania Internetem (IGF).

2. WYNIKI KONSULTACJI Z ZAINTERESOWANYMI STRONAMI ORAZ OCENY SKUTKÓW

2.1. Konsultacje z zainteresowanymi stronami i wykorzystanie wiedzy specjalistycznej

W dniach od 23 lipca do 15 października 2012 r. przeprowadzono internetowe konsultacje społeczne dotyczące zwiększenia bezpieczeństwa sieci i informacji w UE. W sumie Komisja otrzymała 160 odpowiedzi na zamieszczony w internecie kwestionariusz.

Kluczowym wynikiem było stwierdzenie, iż zainteresowane strony na ogół zgodziły się co do konieczności zwiększenia bezpieczeństwa sieci i informacji w całej UE. W szczególności 82,8 % respondentów wyraziło pogląd, że rządy państw członkowskich UE powinny dokładać większych starań w celu zapewnienia wysokiego poziomu bezpieczeństwa sieci i informacji; 82,8 % było zdania, że użytkownicy informacji oraz systemów informatycznych nie są świadomi istniejących zagrożeń i incydentów w odniesieniu do bezpieczeństwa sieci i informacji; 66,3 % zasadniczo opowiedziało się za wprowadzeniem wymogów prawnych w celu przeciwdziałania zagrożeniom w zakresie bezpieczeństwa sieci i informacji; 84,8 % ankietowanych stwierdziło, że wymogi te powinny zostać określone na poziomie UE. Duża część respondentów wyraziła opinię, że wymogi w zakresie bezpieczeństwa sieci i informacji należałoby przyjąć zwłaszcza w odniesieniu do następujących sektorów: bankowość i finanse (91,1 %), energetyka (89,4 %), transport (81,7 %), opieka zdrowotna (89,4 %), usługi internetowe (89,1 %), a także administracja publiczna (87,5 %). Respondenci uznali również, że jeżeli miałby zostać wprowadzony wymóg zgłaszania przypadków naruszenia bezpieczeństwa sieci i informacji właściwemu organowi krajowemu, należałoby go ustanowić na poziomie UE (65,1 %), a także podkreślili, że należałoby nim również objąć administracje publiczne (93,5 %). Respondenci potwierdzili również, że wprowadzenie wymogu wdrożenia nowoczesnych procedur przeciwdziałania zagrożeniom w zakresie bezpieczeństwa sieci i informacji nie wiązałoby się z koniecznością poniesienia znacznych dodatkowych kosztów (63,4 %), oraz że wprowadzenie wymogu zgłaszania przypadków naruszenia bezpieczeństwa również nie oznaczałoby znacznych dodatkowych kosztów (72,3 %).

Konsultacje z państwami członkowskimi przeprowadzono na forum odpowiednich składów Rady, w ramach europejskiego forum państw członkowskich (ang. *European Forum for Member States*, EFMS), podczas konferencji w sprawie cyberbezpieczeństwa zorganizowanej

[21] http://europa.eu/rapid/press-release_MEMO-10-597_pl.htm.

przez służby Komisji oraz Europejskiej Służby Działań Zewnętrznych w dniu 6 lipca 2012 r., oraz w trakcie specjalnych spotkań dwustronnych zwoływanych na wniosek poszczególnych państw członkowskich.

Rozmowy z sektorem prywatnym przeprowadzono w ramach europejskiego partnerstwa publiczno-prywatnego na rzecz odporności[22] oraz w ramach spotkań dwustronnych. Jeśli chodzi o sektor publiczny, Komisja przeprowadziła dyskusje z ENISA i CERT działającym przy instytucjach UE.

2.2. Ocena skutków

Komisja dokonała oceny skutków dla trzech wariantów strategicznych:

Wariant 1: Niepodejmowanie żadnych nowych działań (scenariusz podstawowy): utrzymanie obecnego podejścia;

Wariant 2: Podejście regulacyjne, obejmujące wniosek ustawodawczy w sprawie ustanowienia wspólnych unijnych ram prawnych w zakresie bezpieczeństwa sieci i informacji w odniesieniu do zdolności państw członkowskich, mechanizmów współpracy na poziomie UE oraz wymogów dla najważniejszych podmiotów prywatnych i organów administracji publicznej;

Wariant 3: Podejście mieszane, w ramach którego dobrowolne inicjatywy dotyczące zdolności państw członkowskich w zakresie bezpieczeństwa sieci i informacji oraz mechanizmów współpracy na poziomie UE połączone są z wprowadzeniem wymogów regulacyjnych dla najważniejszych podmiotów prywatnych i organów administracji publicznej.

Komisja stwierdziła, że wariant 2 będzie miał największy pozytywny wpływ, gdyż doprowadzi do znacznego zwiększenia ochrony konsumentów, przedsiębiorstw i rządów w UE przed incydentami w zakresie bezpieczeństwa sieci i informacji. W szczególności zobowiązania nałożone na państwa członkowskie zapewnią odpowiednie przygotowanie na poziomie krajowym i przyczynią się do wytworzenia klimatu wzajemnego zaufania, co jest niezbędnym warunkiem skutecznej współpracy na poziomie UE. Ustanowienie mechanizmów współpracy na poziomie UE za pośrednictwem odpowiedniej sieci umożliwiłoby zapobieganie transgranicznym incydentom i zagrożeniom w zakresie bezpieczeństwa sieci i informacji oraz reagowanie na nie w spójny i skoordynowany sposób. Wprowadzenie wymogów wdrożenia strategii przeciwdziałania zagrożeniom w zakresie bezpieczeństwa sieci i informacji dla organów administracji publicznej i najważniejszych podmiotów prywatnych stworzyłoby silną zachętę do efektywnego przeciwdziałania zagrożeniom związanym z bezpieczeństwem. Wprowadzenie obowiązku zgłaszania incydentów w zakresie bezpieczeństwa sieci i informacji mających znaczące konsekwencje zwiększyłoby zdolność reagowania na incydenty oraz zapewniłoby większą przejrzystość. Ponadto poprzez uporządkowanie sytuacji u siebie UE będzie mogła rozszerzyć swoje wpływy w kontekście międzynarodowym, dzięki czemu stałaby się jeszcze bardziej wiarygodnym partnerem do współpracy na poziomie dwustronnym i wielostronnym. UE będzie więc również mieć możliwość skuteczniejszego promowania praw podstawowych i wartości leżących u podstaw UE za granicą.

Ocena ilościowa wykazała, że wariant 2 nie nałoży nieproporcjonalnych obciążeń na państwa członkowskie. Koszty ponoszone przez sektor prywatny będą również ograniczone ze względu na fakt, że wiele podmiotów spełnia już obowiązujące wymogi bezpieczeństwa (tzn.

[22] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

zobowiązanie administratorów danych do podjęcia środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa danych osobowych, w tym środków w zakresie bezpieczeństwa sieci i informacji). Uwzględniono również obecne wydatki na bezpieczeństwo w sektorze prywatnym.

Niniejszy wniosek jest zgodny z zasadami uznanymi w Karcie praw podstawowych Unii Europejskiej, w szczególności z prawem do poszanowania życia prywatnego i komunikowania się, prawem do ochrony danych osobowych i wolności prowadzenia działalności gospodarczej, prawem własności, prawem do skutecznego środka prawnego i prawem do bycia wysłuchanym. Niniejszą dyrektywę należy wdrażać zgodnie z tymi prawami i zasadami.

3. ASPEKTY PRAWNE WNIOSKU

3.1. Podstawa prawna

Unia Europejska jest uprawniona do przyjmowania środków w celu ustanowienia lub zapewnienia funkcjonowania rynku wewnętrznego zgodnie z odpowiednimi postanowieniami Traktatów (art. 26 Traktatu o funkcjonowaniu Unii Europejskiej – TFUE). Zgodnie z art. 114 TFUE UE może przyjąć „środki dotyczące zbliżenia przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich, które mają na celu ustanowienie i funkcjonowanie rynku wewnętrznego".

Jak wskazano powyżej, sieci i systemy informatyczne odgrywają istotną rolę w ułatwianiu transgranicznego przepływu towarów, usług i osób. Często są one ze sobą wzajemnie powiązane, a internet ma charakter globalny. Ze względu na ten nieunikniony wymiar ponadnarodowy zakłócenia w jednym państwie członkowskim mogą mieć również wpływ na inne państwa członkowskie oraz na UE jako całość. Odporność i stabilność sieci i systemów informatycznych mają zatem zasadnicze znaczenie dla zapewnienia sprawnego funkcjonowania rynku wewnętrznego.

Prawodawca unijny uznał już konieczność harmonizacji przepisów w zakresie bezpieczeństwa sieci i informacji w celu zapewnienia rozwoju rynku wewnętrznego. W szczególności miało to miejsce w przypadku rozporządzenia (WE) nr 460/2004 ustanawiającego ENISA[23], które opiera się na art. 114 TFUE.

Różnice wynikające z nierównych krajowych zdolności w zakresie bezpieczeństwa sieci i informacji, niejednolitej polityki oraz nierównego poziomu ochrony w poszczególnych państwach członkowskich prowadzą do powstania barier na rynku wewnętrznym i uzasadniają podjęcie działań na poziomie UE.

3.2. Pomocniczość

Podjęcie działań w dziedzinie bezpieczeństwa sieci i informacji na poziomie europejskim jest zgodne z zasadą pomocniczości.

Po pierwsze, uwzględniając transgraniczny charakter kwestii bezpieczeństwa sieci i informacji, niepodjęcie działań na poziomie UE doprowadziłoby do sytuacji, w której każde państwo członkowskie działałoby w pojedynkę, pomijając przy tym współzależność między sieciami i systemami informatycznymi w UE. Odpowiedni stopień koordynacji między państwami członkowskimi zapewni właściwe przeciwdziałanie zagrożeniom w zakresie bezpieczeństwa sieci i informacji w kontekście transgranicznym, w którym zagrożenia te występują. Różnice w uregulowaniach dotyczących bezpieczeństwa sieci i informacji

[23] Rozporządzenie (WE) nr 460/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (Dz.U. L 77 z 13.3.2004, s. 1).

stanowią przeszkodę dla przedsiębiorstw, które chcą prowadzić działalność w kilku krajach, oraz utrudniają osiągnięcie globalnych korzyści skali.

Po drugie, wprowadzenie wymogów prawnych na poziomie UE jest potrzebne, aby stworzyć równe warunki działania i usunąć luki prawne. Przyjęcie podejścia opartego wyłącznie na dobrowolności doprowadziło do współpracy jedynie w przypadku będących w mniejszości państw członkowskich posiadających wysoki poziom zdolności. W celu zaangażowania wszystkich państw członkowskich należy doprowadzić do sytuacji, w której wszystkie te państwa posiadają wymagany minimalny poziom zdolności. Środki w zakresie bezpieczeństwa sieci i informacji przyjmowane przez rządy muszą być spójne i skoordynowane, tak aby możliwe było opanowanie i zminimalizowanie skutków incydentów w zakresie bezpieczeństwa sieci i informacji. W ramach sieci, poprzez wymianę najlepszych praktyk i przy ciągłym zaangażowaniu ENISA, właściwe organy i Komisja będą współpracować w celu ułatwienia spójnego wdrożenia dyrektywy w całej UE. Ponadto wspólne działania w zakresie polityki dotyczącej bezpieczeństwa sieci i informacji mogą mieć istotny korzystny wpływ na skuteczną ochronę praw podstawowych, a zwłaszcza prawa do ochrony danych osobowych i prywatności. Działania na poziomie UE przyczynią się zatem do poprawy skuteczności obowiązujących krajowych strategii i ułatwią ich dalszy rozwój.

Proponowane środki są również zgodne z zasadą proporcjonalności. Wymogi dla państw członkowskich ustanowione są na minimalnym poziomie, który jest niezbędny do osiągnięcia odpowiedniej gotowości i umożliwienia współpracy opartej na zaufaniu. Umożliwia to również państwom członkowskim uwzględnienie uwarunkowań krajowych oraz zapewnia stosowanie wspólnych zasad UE w proporcjonalny sposób. Szeroki zakres zastosowania umożliwi państwom członkowskim wdrożenie dyrektywy w świetle rzeczywistych zagrożeń występujących na poziomie krajowym, które określone będą w krajowej strategii bezpieczeństwa sieci i informacji. Wymogi dotyczące wdrożenia strategii przeciwdziałania zagrożeniom obejmują tylko podmioty o znaczeniu krytycznym i przewidują wprowadzenie środków, które są proporcjonalne do zagrożenia. W ramach konsultacji społecznych podkreślono znaczenie zapewnienia bezpieczeństwa tych podmiotów o znaczeniu krytycznym. Wymogi dotyczące zgłaszania incydentów będą dotyczyć jedynie incydentów mających znaczące skutki. Jak wskazano powyżej, środki te nie nakładają nieproporcjonalnych kosztów, ponieważ będąc administratorami danych, wiele z tych podmiotów podlega już obowiązującym przepisom dotyczącym ochrony danych w celu zapewnienia ochrony danych osobowych.

Aby uniknąć nakładania nieproporcjolanych obciążeń na małe podmioty, zwłaszcza MŚP, wymogi są proporcjonalne do zagrożeń dla danej sieci lub danego systemu informatycznego i nie powinny mieć zastosowania do mikroprzedsiębiorstw. Zagrożenia będą określane w pierwszej kolejności przez podmioty podlegające tym wymogom, które same będą musiały podejmować decyzje w sprawie przyjęcia środków ograniczenia tych zagrożeń.

W związku z aspektami transgranicznymi incydentów i zagrożeń w zakresie bezpieczeństwa sieci i informacji wyznaczone cele mogą zostać lepiej osiągnięte na poziomie UE niż poprzez działania samych państw członkowskich. UE może zatem przyjąć środki zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności proponowana dyrektywa nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

Aby osiągnąć te cele, Komisja powinna być uprawniona do przyjmowania aktów delegowanych zgodnie z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej w celu uzupełniania i zmieniania niektórych, innych niż istotne, elementów aktu podstawowego.

Wniosek Komisji ma również na celu zapewnienie proporcjonalności w procesie nakładania wymogów na podmioty prywatne i publiczne.

W celu zapewnienia jednolitych warunków wdrażania aktu podstawowego Komisja powinna być uprawniona do przyjmowania aktów wykonawczych zgodnie z art. 291 Traktatu o funkcjonowaniu Unii Europejskiej.

Uwzględniając w szczególności szeroki zakres proponowanej dyrektywy oraz fakt, że dotyczy ona ściśle regulowanych obszarów, a także z uwagi na zobowiązania prawne wynikające z jej rozdziału IV, do zgłoszenia środków transpozycji powinny być dołączone dokumenty wyjaśniające. Zgodnie ze wspólną deklaracją polityczną państw członkowskich i Komisji z dnia 28 września 2011 r. dotyczącą dokumentów wyjaśniających 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.

4. WPŁYW NA BUDŻET

Współpraca i wymiana informacji między państwami członkowskimi powinna się odbywać za pomocą bezpiecznej infrastruktury. Wniosek będzie miał wpływ na budżet UE tylko w sytuacji, gdy państwa członkowskie postanowią dostosować istniejącą infrastrukturę (np. sTESTA) i gdy powierzą Komisji realizację tego zadania w ramach wieloletnich ram finansowych na lata 2014–2020. Jednorazowy koszt, szacowany na 1 250 000 EUR, będzie pokryty z budżetu UE, pozycja budżetowa 09.03.02 (wspieranie wzajemnych połączeń i interoperacyjności krajowych usług publicznych świadczonych online, a także dostępu do takich sieci – rozdział 09.03, instrument „Łącząc Europę” – sieci telekomunikacyjne), pod warunkiem że w ramach instrumentu „Łącząc Europę” dostępna będzie wystarczająca ilość środków. W przeciwnym wypadku państwa członkowskie mogą podzielić się jednorazowym kosztem dostosowania istniejącej infrastruktury, bądź też mogą podjąć decyzję o utworzeniu nowej infrastruktury i poniesieniu kosztów, które szacuje się na około 10 mln EUR rocznie.

2013/0027 (COD)

Wniosek

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

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

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 114,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[1],

po konsultacji z Europejskim Inspektorem Ochrony Danych,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(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.

(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.

(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.

(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

[1] Dz.U. C […] z […], s. […].

również w odniesieniu do organów administracji publicznej i operatorów krytycznej infrastruktury teleinformatycznej.

(5) W celu uwzględnienia wszystkich istotnych incydentów i zagrożeń niniejsza dyrektywa powinna mieć zastosowanie do wszystkich sieci i systemów informatycznych. Obowiązki nałożone na organy administracji publicznej i podmioty gospodarcze nie powinny mieć jednak zastosowania w odniesieniu do przedsiębiorstw udostępniających publiczne sieci łączności lub świadczących publicznie dostępne usługi łączności elektronicznej w rozumieniu dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa)[2], które podlegają szczególnym wymogom w zakresie bezpieczeństwa i integralności ustanowionym w art. 13a tej dyrektywy, ani nie powinny mieć zastosowania w odniesieniu do dostawców usług zaufania.

(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.

(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.

(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.

(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.

(10) W celu umożliwienia skutecznego wprowadzenia w życie przepisów przyjętych zgodnie z niniejszą dyrektywą w każdym państwie członkowskim należy ustanowić

[2] Dz.U. L 108 z 24.4.2002, s. 33.

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.

(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.

(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.

(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.

(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.

(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.

(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.

(17) 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.

(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.

(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.

(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.

(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.

(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.

(23) Dyrektywa 2002/21/WE wymaga, by przedsiębiorstwa udostępniające publiczne sieci łączności elektronicznej lub świadczące publicznie dostępne usługi łączności elektronicznej podejmowały odpowiednie środki w celu zabezpieczenia integralności i bezpieczeństwa oraz wprowadza wymogi dotyczące zgłaszania przypadków naruszeń bezpieczeństwa i utraty integralności. Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o

prywatności i łączności elektronicznej)[3] wymaga od dostawcy publicznie dostępnych usług łączności elektronicznej podjęcia właściwych środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa oferowanych przez siebie usług.

(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[4], 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 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.

(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.

(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 innym podmiotom.

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

(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

[3] Dz.U. L 201 z 31.7.2002, s. 37.
[4] Dz.U. L 204 z 21.7.1998, s. 37.

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.

(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.

(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.

(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[5]. 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.

(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,

[5] SEC(2012) 72 final.

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[6].

(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.

(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.

(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.

(36) W celu zapewnienia jednolitych warunków wykonywania niniejszej dyrektywy należy powierzyć Komisji uprawnienia wykonawcze w zakresie współpracy między właściwymi organami i Komisją w ramach sieci współpracy, dostępu do bezpiecznej infrastruktury służącej do wymiany informacji, unijnego planu współpracy w zakresie bezpieczeństwa sieci i informacji, formatów i procedur mających zastosowanie wobec wymogów dotyczących informowania społeczeństwa o incydentach, oraz norm lub specyfikacji technicznych dotyczących bezpieczeństwa sieci i informacji. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiającym przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję[7].

(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.

(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.

(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

[6] Dz.U. L 316 z 14.11.2012, s. 12.
[7] Dz.U. L 55 z 28.2.2011, s. 13.

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[8]. 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.

(40) Ponieważ cel niniejszej dyrektywy, to jest zapewnienie wysokiego poziomu bezpieczeństwa sieci i informacji w Unii, nie może zostać osiągnięty w wystarczającym stopniu przez państwa członkowskie działające samodzielnie, natomiast z uwagi na skutki proponowanego działania możliwe jest lepsze jego osiągnięcie na poziomie unijnym, Unia może podjąć działania zgodnie z zasadą pomocniczości, o której mowa w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsza dyrektywa nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

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

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot i zakres zastosowania

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

2. W tym celu niniejsza dyrektywa:

a) określa obowiązki dla wszystkich państw członkowskich w zakresie zapobiegania zagrożeniom i incydentom dotyczącym sieci i systemów informatycznych, postępowania w przypadku ich wystąpienia 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 i sprawnego postępowania w przypadku wystąpienia zagrożeń i incydentów dotyczących sieci i systemów informatycznych oraz reagowania na nie;

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

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

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

4. Niniejszą dyrektywę stosuje się bez uszczerbku dla unijnych przepisów dotyczących cyberprzestępczości oraz dyrektywy Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony[9].

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[10], 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[11].

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.

Artykuł 2

Minimalna harmonizacja

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

Artykuł 3

Definicje

Do celów niniejszej dyrektywy stosuje się następujące definicje:

1) „sieci i systemy informatyczne” oznaczają:

   a) sieci łączności elektronicznej w rozumieniu dyrektywy 2002/21/WE, oraz

   b) wszelkie urządzenia lub grupy połączonych lub powiązanych urządzeń, z których jedno lub więcej, zgodnie z oprogramowaniem, dokonuje automatycznego przetwarzania danych komputerowych, jak również

[9] Dz.U. L 345 z 23.12.2008, s. 75.
[10] Dz.U. L 281 z 23.11.1995, s. 31.
[11] SEC(2012) 72 final.

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

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;

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

4) „incydent” oznacza każdą okoliczność lub zdarzenie, które mają rzeczywisty niekorzystny wpływ na bezpieczeństwo;

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

6) „plan współpracy w zakresie bezpieczeństwa sieci i informacji” oznacza plan zawierający ramy dla funkcji, obowiązków i procedur organizacyjnych mających na celu utrzymanie lub przywrócenie funkcjonowania sieci i systemów informatycznych, w przypadku wystąpienia zagrożenia lub incydentu, które ich dotyczą;

7) „postępowanie w przypadku incydentu” oznacza wszystkie procedury umożliwiające analizę i ograniczenie skutków incydentu oraz reakcję na niego;

8) „podmiot gospodarczy” oznacza:

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.

9) „norma” oznacza normę, o której mowa w rozporządzeniu (UE) nr 1025/2012;

10) „specyfikacja” oznacza specyfikację, o której mowa w rozporządzeniu (UE) nr 1025/2012;

11) „dostawca usług zaufania” oznacza każdą osobę fizyczną lub prawną, która świadczy jakąkolwiek elektroniczną usługę polegającą na tworzeniu, kontroli, walidacji i przechowywaniu podpisów elektronicznych, pieczęci elektronicznych, elektronicznych znaczników czasu, dokumentów elektronicznych, usług doręczenia elektronicznego, usług uwierzytelniania witryn internetowych i certyfikatów elektronicznych, w tym certyfikatów podpisów elektronicznych i pieczęci elektronicznych.

ROZDZIAŁ II

RAMY KRAJOWE W ZAKRESIE BEZPIECZEŃSTWA SIECI I INFORMACJI

Artykuł 4

Zasada

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

Artykuł 5

Krajowa strategia w zakresie bezpieczeństwa sieci i informacji oraz krajowy plan współpracy w zakresie bezpieczeństwa sieci i informacji

1. Każde państwo członkowskie przyjmuje krajową strategię w zakresie bezpieczeństwa sieci i informacji określającą cele strategiczne i konkretne środki polityczne i regulacyjne mające na celu osiągnięcie i utrzymanie wysokiego poziomu bezpieczeństwa sieci i informacji. Krajowa strategia w zakresie bezpieczeństwa sieci i informacji uwzględnia zwłaszcza następujące kwestie:

a) określenie celów i priorytetów strategii w oparciu o aktualną analizę zagrożeń i incydentów;

b) ramy zarządzania służące realizacji celów i priorytetów strategii, w tym jasne określenie funkcji i zakresu obowiązków organów rządowych i innych właściwych podmiotów;

c) określenie ogólnych środków w zakresie gotowości, reagowania i przywracania stanu normalnego, w tym mechanizmów współpracy pomiędzy sektorami publicznym i prywatnym;

d) wstępne określenie programów edukacyjnych, informacyjnych i szkoleniowych;

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

2. Krajowa strategia w zakresie bezpieczeństwa sieci i informacji obejmuje krajowy plan współpracy w zakresie bezpieczeństwa sieci i informacji, spełniający co najmniej następujące wymogi:

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

b) określenie funkcji i zakresu obowiązków poszczególnych podmiotów zaangażowanych w realizację planu;

c) określenie procedur współpracy i komunikacji zapewniających zapobieganie, wykrywanie, reagowanie, naprawę i przywrócenie stanu normalnego, dostosowanych do poziomu stanu alarmowego;

d) opracowanie planu dotyczącego ćwiczeń i szkoleń w zakresie bezpieczeństwa sieci i informacji, mającego na celu ulepszenie, zatwierdzenie i sprawdzenie planu. Wyciągnięte wnioski są udokumentowywane i włączane do zaktualizowanych wersji planu.

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.

Artykuł 6

Właściwy organ krajowy ds. bezpieczeństwa sieci i systemów informatycznych

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

2. Właściwe organy monitorują stosowanie niniejszej dyrektywy na poziomie krajowym oraz przyczyniają się do jej jednolitego stosowania w całej Unii.

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.

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.

5. W stosownych przypadkach właściwe organy konsultują się i współpracują z odpowiednimi krajowymi organami ścigania i z organami ochrony danych.

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.

Artykuł 7

Zespół reagowania na incydenty komputerowe

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.

2. Państwa członkowskie zapewniają CERT odpowiednie zasoby techniczne, finansowe i ludzkie, aby mogły one skutecznie realizować zadania określone w załączniku I pkt 2.

3. Państwa członkowskie dopilnowują, by CERT wykorzystywały bezpieczną i odporną infrastrukturę komunikacyjną i informacyjną na poziomie krajowym, która jest kompatybilna i interoperacyjna z bezpiecznym systemem wymiany informacji, o którym mowa w art. 9.

4. Państwa członkowskie powiadamiają Komisję o zasobach i mandacie CERT, jak również o ich procedurach postępowania w przypadku incydentów.

5. CERT działa pod nadzorem właściwego organu, który regularnie dokonuje przeglądu stosowności jego zasobów, jego mandatu oraz skuteczności jego procedury postępowania w przypadku incydentów.

ROZDZIAŁ III

WSPÓŁPRACA MIĘDZY WŁAŚCIWYMI ORGANAMI

Artykuł 8

Sieć współpracy

1. Właściwe organy i Komisja ustanawiają sieć („sieć współpracy”) służącą do współpracy 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.

3. W ramach sieci współpracy właściwe organy:

   a) przekazują wczesne ostrzeżenia dotyczące zagrożeń i incydentów zgodnie z art. 10;

   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;

   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;

   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;

   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.

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.

Artykuł 9

Bezpieczny system wymiany informacji

1. Wymiana szczególnie chronionych i poufnych informacji w ramach sieci współpracy odbywa się za pośrednictwem bezpiecznej infrastruktury.

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:

   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.

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.

Artykuł 10

Wczesne ostrzeżenia

1. W ramach sieci współpracy właściwe organy 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;

   c) mają one wpływ lub mogą mieć 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.

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.

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.

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.

Artykuł 11

Skoordynowana reakcja

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.

2. Informacje o różnych środkach przyjętych na poziomie krajowym w wyniku skoordynowanej reakcji przekazuje się do sieci współpracy.

Artykuł 12

Unijny plan współpracy w zakresie bezpieczeństwa sieci i informacji

1. Komisja jest uprawniona do przyjęcia, w drodze aktów wykonawczych, unijnego planu współpracy w zakresie bezpieczeństwa sieci i informacji. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 19 ust. 3.

2. Unijny plan współpracy w zakresie bezpieczeństwa sieci i informacji obejmuje:

   a) do celów art. 10:

      – określenie formatu i procedur gromadzenia i wymiany kompatybilnych i porównywalnych informacji na temat zagrożeń i incydentów przez właściwe organy;

      – określenie procedur i kryteriów oceny zagrożeń i incydentów przez sieć współpracy;

   b) procedury, jakie należy stosować w przypadku skoordynowanych reakcji na mocy art. 11, w tym określenie funkcji i obowiązków oraz procedur współpracy;

   c) plan działania dotyczący ćwiczeń i szkoleń w zakresie bezpieczeństwa sieci i informacji, mający na celu wzmocnienie, zatwierdzenie i sprawdzenie głównego planu;

   d) program dotyczący transferu wiedzy między państwami członkowskimi w odniesieniu do budowy zdolności i wzajemnego uczenia się;

   e) program dotyczący działań informacyjnych i szkoleń między państwami członkowskimi.

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.

Artykuł 13

Współpraca międzynarodowa

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.

ROZDZIAŁ IV

BEZPIECZEŃSTWO SIECI I SYSTEMÓW INFORMATYCZNYCH ORGANÓW ADMINISTRACJI PUBLICZNEJ I PODMIOTÓW GOSPODARCZYCH

Artykuł 14

Wymogi w zakresie bezpieczeństwa i zgłaszanie incydentów

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.

3. Wymogi zawarte w ust. 1 i 2 stosuje się do wszystkich podmiotów gospodarczych świadczących usługi w obrębie Unii Europejskiej.

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

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.

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[12].

Artykuł 15

Wdrażanie i egzekwowanie

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.

[12] Dz.U. L 124 z 20.5.2003, s. 36.

2. Państwa członkowskie zapewniają właściwym organom uprawnienia, na podstawie których mogą one wymagać od podmiotów gospodarczych i organów administracji publicznej:

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.

3. Państwa członkowskie zapewniają właściwym organom uprawnienia do wydawania wiążących instrukcji dla podmiotów gospodarczych i organów administracji publicznej.

4. Właściwe organy zgłaszają organom ścigania poważne incydenty, 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.

6. Państwa członkowskie zapewniają możliwość poddania kontroli sądowej wszelkich obowiązków nałożonych na organy administracji publicznej oraz podmioty gospodarcze na mocy niniejszego rozdziału.

Artykuł 16

Normalizacja

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

2. Komisja sporządza – w drodze aktów wykonawczych – wykaz norm, o których mowa w ust. 1. Wykaz ten zostaje opublikowany w *Dzienniku Urzędowym Unii Europejskiej*.

ROZDZIAŁ V

PRZEPISY KOŃCOWE

Artykuł 17

Sankcje

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.

2. Państwa członkowskie dopilnowują, by w przypadku incydentów zagrażających bezpieczeństwu danych osobowych przewidziane sankcje były zgodne z sankcjami przewidzianymi w rozporządzeniu Parlamentu Europejskiego i Rady w sprawie

ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych[13].

Artykuł 18

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.

Artykuł 19

Procedura komitetowa

1. Komisję wspomaga komitet (Komitet ds. Bezpieczeństwa Sieci i Informacji). Komitet jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

2. W przypadku odesłania do niniejszego ustępu stosuje się art. 4 rozporządzenia (UE) nr 182/2011.

3. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

Artykuł 20

Przegląd

Komisja dokonuje okresowego przeglądu funkcjonowania niniejszej dyrektywy i składa Parlamentowi Europejskiemu i Radzie sprawozdania na ten temat. Pierwsze sprawozdanie

[13] SEC(2012) 72 final.

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.

Artykuł 21

Transpozycja

4. Państwa członkowskie przyjmują i publikują, najpóźniej do dnia [półtora roku po przyjęciu] r., przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy. Niezwłocznie przekazują Komisji tekst tych przepisów.

   Państwa członkowskie stosują te przepisy od dnia [półtora roku po przyjęciu] r.

   Przepisy przyjęte przez państwa członkowskie zawierają odniesienie do niniejszej dyrektywy lub odniesienie takie towarzyszy ich urzędowej publikacji. Metody dokonywania takiego odniesienia określane są przez państwa członkowskie.

5. Państwa członkowskie przekazują Komisji tekst podstawowych przepisów prawa krajowego, przyjętych w dziedzinie objętej niniejszą dyrektywą.

Artykuł 22

Wejście w życie

Niniejsza dyrektywa wchodzi w życie [dwudziestego] dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 23

Adresaci

Niniejsza dyrektywa skierowana jest do państw członkowskich.

Sporządzono w Brukseli dnia […] r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodniczący	*Przewodniczący*

ZAŁĄCZNIK I

Zespoły reagowania na incydenty komputerowe (CERT) – wymogi i zadania

Wymogi i zadania dla CERT są odpowiednio i jasno określone i umocowane w strategiach lub regulacjach krajowych. Obejmują one następujące elementy:

(1) Wymogi dotyczące CERT

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.

b) CERT wdraża środki mające na celu zapewnienie poufności, integralności, dostępności i wiarygodności otrzymywanych i przetwarzanych informacji, oraz zarządza tymi środkami.

c) Biura CERT oraz wspierające systemy informatyczne są zlokalizowane w bezpiecznych miejscach.

d) W celu monitorowania działalności CERT i zapewnienia jej ciągłej poprawy należy utworzyć system zarządzania jakością usług. System ten jest oparty na jasno zdefiniowanych metodach pomiaru, które obejmują formalne poziomy usług oraz kluczowe wskaźniki wyników.

e) Ciągłość działania:

- CERT musi być wyposażony w odpowiedni system zarządzania i dysponowania wnioskami w celu ułatwienia ich późniejszego przekazywania.
- CERT dysponuje wystarczającą liczbą personelu, aby zapewnić nieprzerwaną dostępność usług.
- CERT korzysta z infrastruktury o gwarantowanej ciągłości działania. W tym kontekście należy zapewnić CERT systemy redundantne oraz rezerwowy lokal w celu zapewnienia stałego dostępu do środków komunikacji.

(2) Zadania CERT

a) Zadania CERT obejmują co najmniej:

- monitorowanie incydentów na poziomie krajowym;
- przekazywanie zainteresowanym stronom wczesnych ostrzeżeń, ogłaszanie alarmów, wydawanie ogłoszeń i przekazywanie informacji skierowanych do zainteresowanych stron i dotyczących zagrożeń oraz incydentów;
- reagowanie na incydenty;
- zapewnianie dynamicznej analizy zagrożeń i incydentów oraz zintegrowanej oceny sytuacji;
- informowanie opinii publicznej o zagrożeniach związanych z działalnością online,
- organizowanie kampanii w zakresie bezpieczeństwa sieci i informacji.

b) CERT nawiązuje współpracę z sektorem prywatnym.

c) W celu ułatwienia współpracy CERT wspiera przyjmowanie i wykorzystywanie wspólnych lub znormalizowanych praktyk w odniesieniu do:

- procedur postępowania w przypadku wystąpienia incydentów i zagrożeń;
- systemów klasyfikacji incydentów, zagrożeń i informacji;
- taksonomii metod pomiarów;
- formatów wymiany informacji dotyczących zagrożeń i incydentów oraz konwencji nazewnictwa systemów.

ZAŁĄCZNIK II

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):

1. Energetyka

- dostawcy energii elektrycznej i gazu
- operatorzy systemów dystrybucyjnych energii elektrycznej lub gazu oraz detaliści sprzedający energię elektryczną lub gaz konsumentom końcowym
- operatorzy systemów przesyłowych gazu ziemnego, operatorzy systemu magazynowania i operatorzy systemów LNG
- operatorzy systemów przesyłowych energii elektrycznej
- podmioty eksploatujące rurociągi przesyłowe i magazyny ropy naftowej
- podmioty działające na rynku gazu i energii elektrycznej
- operatorzy instalacji służących do produkcji ropy naftowej i gazu ziemnego, obiekty służące do rafinacji i przetwarzania

2. Transport

- przewoźnicy lotniczy (przewozy pasażerskie i towarowe)
- przewoźnicy morscy (przedsiębiorstwa świadczące usługi pasażerskiego transportu morskiego i przybrzeżnego oraz przedsiębiorstwa świadczące usługi towarowego transportu morskiego i przybrzeżnego)
- koleje (zarządcy infrastruktury, przedsiębiorstwa zintegrowane oraz przedsiębiorstwa transportu kolejowego)
- porty lotnicze
- porty
- operatorzy zarządzający ruchem
- pomocnicze usługi logistyczne: a) magazynowanie oraz składowanie, b) przeładunek i c) pozostała działalność wspomagająca transport

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

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

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

1.2. Dziedzina(-y) polityki w strukturze ABM/ABB, których dotyczy wniosek/inicjatywa

1.3. Charakter wniosku/inicjatywy

1.4. Cele

1.5. Uzasadnienie wniosku/inicjatywy

1.6. Czas trwania działania i jego wpływ finansowy

1.7. Przewidywany(-e) tryb(-y) zarządzania

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

2.2. System zarządzania i kontroli

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Dział(y) wieloletnich ram finansowych i pozycja(pozycje) wydatków w budżecie, na które wniosek/inicjatywa ma wpływ

3.2. Szacunkowy wpływ na wydatki

3.2.1. Synteza szacunkowego wpływu na wydatki

3.2.2. Szacunkowy wpływ na środki operacyjne

3.2.3. Szacunkowy wpływ na środki administracyjne

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

3.2.5. Udział osób trzecich w finansowaniu

3.3. Szacunkowy wpływ na dochody

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii

1.2. Dziedzina(-y) polityki w strukturze ABM/ABB, których dotyczy wniosek/inicjatywa[37]

- 09 – Sieci komunikacyjne, treści i technologie

1.3. Charakter wniosku/inicjatywy

☒ Wniosek/inicjatywa dotyczy **nowego działania**

☐ Wniosek/inicjatywa dotyczy **nowego działania będącego następstwem projektu pilotażowego/działania przygotowawczego**[38]

☐ Wniosek/inicjatywa wiąże się z **przedłużeniem bieżącego działania**

☐ Wniosek/inicjatywa dotyczy **działania, które zostało przekształcone pod kątem nowego działania**

1.4. Cele

1.4.1. Wieloletni(e) cel(e) strategiczny(-e) Komisji wskazany(-e) we wniosku/inicjatywie

Celem proponowanej dyrektywy jest zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji (ang. *network and information security*, NIS) w całej UE.

1.4.2. Cel szczegółowy i działanie ABM/ABB, których dotyczy wniosek/inicjatywa

Wniosek ustanawia środki w celu zapewnienia wspólnego wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii.

Cele szczegółowe obejmują:

1. zapewnienie minimalnego poziomu bezpieczeństwa sieci i informacji w państwach członkowskich, a tym samym zwiększenie ogólnego poziomu gotowości i reagowania;

2. poprawę współpracy w zakresie bezpieczeństwa sieci i informacji na poziomie UE w celu efektywnego zwalczania incydentów i zagrożeń transgranicznych. Aby umożliwić wymianę szczególnie chronionych i poufnych informacji, zapewniona zostanie bezpieczna infrastruktura do wymiany informacji między właściwymi organami;

3. stworzenie kultury wspierającej przeciwdziałanie zagrożeniom i usprawnienie wymiany informacji między sektorem prywatnym i publicznym.

Działanie(-a) ABM/ABB, którego(-ych) dotyczy wniosek/inicjatywa

Dyrektywa dotyczy podmiotów (przedsiębiorstw i organizacji, w tym MŚP) w kilku sektorach (energetyka, transport, instytucje kredytowe oraz giełdy papierów wartościowych, opieka zdrowotna i technologie będące podstawą kluczowych usług internetowych), a także organów administracji publicznej. Dyrektywa uwzględnia powiązania z organami ścigania i ochrony danych oraz uwzględnia aspekty bezpieczeństwa sieci i informacji w stosunkach zewnętrznych.

---

[37] ABM: Activity Based Management: zarządzanie kosztami działań - ABB: Activity Based Budgeting: budżet zadaniowy.

[38] O którym mowa w art. 49 ust. 6 lit. a) lub b) rozporządzenia finansowego.

– 09 – Sieci komunikacyjne, treści i technologie

– 02 – Przedsiębiorstwa

– 32 – Energetyka

– 06 – Mobilność i transport

– 17 – Ochrona zdrowia i konsumentów

– 18 – Sprawy wewnętrzne

– 19 – Działania zewnętrzne

– 33 – Sprawiedliwość

– 12 – Rynek wewnętrzny

1.4.3. Oczekiwany(-e) wynik(i) i wpływ

Należy wskazać, jakie efekty przyniesie wniosek/inicjatywa beneficjentom/grupie docelowej.

Nastąpi znaczna poprawa ochrony konsumentów, przedsiębiorstw i administracji rządowych w UE przed incydentami i zagrożeniami w zakresie bezpieczeństwa sieci i informacji.

Szczegółowe informacje znajdują się w pkt 8.2 („Wpływ wariantu 2 – Podejście regulacyjne) w dołączonym do niniejszego wniosku ustawodawczego dokumencie roboczym służb Komisji zawierającym ocenę skutków.

1.4.4. Wskaźniki wyników i wpływu

Należy określić wskaźniki, które umożliwią monitorowanie realizacji wniosku/inicjatywy.

Wskaźniki monitorowania i oceny znajdują się w pkt 10 oceny skutków.

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Potrzeba(-y), która(-e) ma(-ją) zostać zaspokojona(-e) w perspektywie krótko- lub długoterminowej

Każde państwo członkowskie będzie zobowiązane posiadać:

- krajową strategię w zakresie bezpieczeństwa sieci i informacji;

- plan współpracy w zakresie bezpieczeństwa sieci i informacji;

- właściwy organ krajowy ds. bezpieczeństwa sieci i informacji; oraz

- zespół reagowania na incydenty komputerowe (CERT).

Na poziomie UE państwa członkowskie będą zobowiązane do współpracy za pośrednictwem sieci.

Organy administracji publicznej oraz najważniejsze podmioty prywatne będą zobowiązane do przeciwdziałania zagrożeniom dotyczącym bezpieczeństwa sieci i informacji oraz do zgłaszania właściwym organom incydentów w zakresie bezpieczeństwa sieci i informacji o znaczących skutkach.

1.5.2. Wartość dodana z tytułu zaangażowania Unii Europejskiej

Ze względu na transgraniczny charakter kwestii związanych z bezpieczeństwem sieci i informacji różnice w stosownych uregulowaniach prawnych stanowią przeszkodę dla przedsiębiorstw, które chcą prowadzić działalność w wielu krajach, oraz utrudniają osiągnięcie globalnych korzyści skali. Brak działania na poziomie UE mógłby doprowadzić do sytuacji, w której państwa członkowskie działałby w pojedynkę z pominięciem współzależności między sieciami i systemami informatycznymi.

Wytyczone cele mogą zostać lepiej osiągnięte poprzez działania na poziomie UE niż poprzez działania podejmowane tylko na poziomie państw członkowskich.

1.5.3. Główne wnioski wyciągnięte z podobnych działań

Wniosek jest oparty na analizie, z której wynika, że w celu zapewnienia równych warunków działania i usunięcia istniejących luk prawnych konieczne jest wprowadzenie stosownych wymogów prawnych. Przyjęcie w tej dziedzinie podejścia opartego wyłącznie na dobrowolności zapewniło współpracę jedynie w przypadku będących w mniejszości państw członkowskich posiadających wysoki poziom zdolności.

1.5.4. Spójność z innymi właściwymi instrumentami oraz możliwa synergia

Wniosek jest w pełni zgodny z Europejską agenda cyfrową, co oznacza, że jest również zgodny ze strategią „Europa 2020". Ponadto wniosek jest zgodny z unijnymi ramami regulacyjnymi dotyczącymi łączności elektronicznej, dyrektywą UE w sprawie europejskiej infrastruktury krytycznej i dyrektywą UE o ochronie danych, a także stanowi ich uzupełnienie.

Wnioskowi towarzyszy kluczowy dokument, jakim jest komunikat Komisji i Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa w sprawie europejskiej strategii bezpieczeństwa cybernetycznego.

1.6. Czas trwania działania i jego wpływ finansowy

– ☐ Wniosek/inicjatywa o określonym czasie trwania

– ☐ Czas trwania wniosku/inicjatywy: od [DD/MM]RRRR r. do [DD/MM]RRRR r.

– ☐ Czas trwania wpływu finansowego: od RRRR r. do RRRR r.

– ☒ Wniosek/inicjatywa o nieokreślonym czasie trwania

– Okres transpozycji rozpocznie się natychmiast po przyjęciu (szacowanym na 2015 r.) i będzie trwał 18 miesięcy. Wdrażanie dyrektywy rozpocznie się zaraz po jej przyjęciu i będzie obejmować ustanowienie bezpiecznej infrastruktury, która umożliwi współpracę państw członkowskich.

– po którym następuje faza operacyjna.

1.7. Przewidywane tryby zarządzania[39]

– ☒ Bezpośrednie zarządzanie scentralizowane przez Komisję

– ☒ Pośrednie zarządzanie scentralizowane poprzez przekazanie zadań wykonawczych:

– ☐agencjom wykonawczym

– ☒ organom utworzonym przez Wspólnoty[40]

– ☐ krajowym organom publicznym/organom mającym obowiązek świadczenia usługi publicznej

– ☐ osobom odpowiedzialnym za wykonanie określonych działań na mocy tytułu V Traktatu o Unii Europejskiej, określonym we właściwym prawnym akcie podstawowym w rozumieniu art. 49 rozporządzenia finansowego

– ☐ Zarządzanie dzielone z państwami członkowskimi

– ☐ Zarządzanie zdecentralizowane z państwami trzecimi

– ☐ Zarządzanie wspólne z organizacjami międzynarodowymi, w tym Europejską Agencją Kosmiczną

W przypadku wskazania więcej niż jednego trybu, należy podać dodatkowe informacje w części „Uwagi".

Uwagi:

ENISA, która jest zdecentralizowaną agencją utworzoną przez Wspólnoty, może wspomóc państwa członkowskie i Komisję w procesie wdrażania dyrektywy na podstawie udzielonego jej mandatu oraz poprzez przegrupowanie zasobów przewidzianych w ramach wieloletnich ram finansowych na okres 2014–2020 dla tej agencji.

[39] Wyjaśnienia dotyczące trybów zarządzania oraz odniesienia do rozporządzenia finansowego znajdują się na stronie: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.htmlhttp://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[40] O których mowa w art. 185 rozporządzenia finansowego.

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

Należy określić częstotliwość i warunki.

Komisja będzie dokonywać okresowych przeglądów funkcjonowania niniejszej dyrektywy i będzie składać Parlamentowi Europejskiemu i Radzie sprawozdania na ten temat.

Komisja oceni również transpozycję dyrektywy przez państwa członkowskie.

Wniosek w sprawie instrumentu „Łącząc Europę" przewiduje także możliwość przeprowadzenia oceny metod realizacji projektów oraz skutków ich wdrożenia, aby stwierdzić, czy zostały osiągnięte zakładane cele, w tym cele odnoszące się do ochrony środowiska.

2.2. System zarządzania i kontroli

2.2.1. Zidentyfikowane ryzyko

– opóźnienia w realizacji projektów w zakresie budowania bezpiecznej infrastruktury

2.2.2. Przewidywane metody kontroli

Porozumienia i decyzje dotyczące realizacji działań w ramach instrumentu „Łącząc Europę" będą przewidywać nadzór i kontrolę finansową ze strony Komisji lub ze strony upoważnionego przez nią przedstawiciela, a także audyty wykonywane przez Trybunał Obrachunkowy i kontrole na miejscu przeprowadzane przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF).

2.2.3. Koszty i korzyści związane z przeprowadzaniem kontroli i prawdopodobny wskaźnik niezgodności

Kontrole ex ante i ex post oparte na analizie ryzyka oraz możliwość audytu na miejscu zagwarantują, że koszty kontroli będą umiarkowane.

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

Określić istniejące lub przewidywane środki zapobiegania i ochrony

Komisja przyjmuje odpowiednie środki zapewniające, w trakcie realizacji działań finansowanych na podstawie niniejszej dyrektywy, ochronę interesów finansowych Unii przez stosowanie środków zapobiegania nadużyciom finansowym, korupcji i innym nielegalnym działaniom, przez skuteczne kontrole oraz, w razie wykrycia nieprawidłowości, przez odzyskiwanie kwot nienależnie wypłaconych a także, w stosownych przypadkach, przez skuteczne, proporcjonalne i odstraszające kary.

Komisja lub jej przedstawiciele oraz Trybunał Obrachunkowy mają uprawnienia do audytu, na podstawie dokumentacji i na miejscu, wobec wszystkich beneficjentów dotacji, wykonawców i podwykonawców, którzy otrzymują od Unii środki na podstawie niniejszej dyrektywy.

Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) może przeprowadzać kontrole i inspekcje na miejscu u podmiotów gospodarczych, których takie finansowanie bezpośrednio lub pośrednio dotyczy, zgodnie z procedurami określonymi w rozporządzeniu (Euratom, WE) nr 2185/96, w celu ustalenia, czy miały miejsce nadużycie finansowe, korupcja lub jakiekolwiek inne nielegalne działanie, naruszające interesy finansowe Unii, w związku z umową o udzielenie

dotacji, decyzją o udzieleniu dotacji lub zamówieniem dotyczącym finansowania przez Unię.

Bez uszczerbku dla treści powyższych akapitów, w umowach o współpracy z państwami trzecimi i organizacjami międzynarodowymi, umowach o udzielenie dotacji, decyzjach o udzieleniu dotacji i zamówieniach wynikających z wdrożenia niniejszej dyrektywy wyraźnie upoważnia się Komisję, Trybunał Obrachunkowy i OLAF do prowadzenia takich audytów, kontroli i inspekcji na miejscu.

W instrumencie „Łącząc Europę" przewidziano, że umowy dotyczące dotacji i zamówień opierać się będą na standardowych modelach, które określają ogólnie obowiązujące środki zwalczania nadużyć finansowych.

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Dział(y) wieloletnich ram finansowych i pozycja(pozycje) wydatków w budżecie, na które wniosek/inicjatywa ma wpływ

- Istniejące pozycje w budżecie

Według działów wieloletnich ram finansowych i pozycji w budżecie

Dział wieloletnich ram finansowych	Pozycja w budżecie	Rodzaj środków	Wkład			
	Numer [Treść…..…]	Zróżnicowane /niezróżnicowane (41)	państw EFTA[42]	krajów kandydujących[43]	państw trzecich	w rozumieniu art. 18 ust. 1 lit. aa) rozporządzenia finansowego
	09 03 02 Promowanie wzajemnych połączeń i interoperacyjności krajowych usług publicznych świadczonych online, a także dostępu do takich sieci.	Zróżnicowane	NIE	NIE	NIE	NIE

- Nowe pozycje w budżecie, o których utworzenie się wnioskuje (nie dotyczy)

Według działów wieloletnich ram finansowych i pozycji w budżecie

Dział wieloletnich ram finansowych	Pozycja w budżecie	Rodzaj środków	Wkład			
	Numer [treść …..…]	Zróżnicowane /niezróżnicowane	państw EFTA	krajów kandydujących	państw trzecich	w rozumieniu art. 18 ust. 1 lit. aa) rozporządzenia finansowego
	[XX.YY.YY.YY]		TAK/ NIE	TAK/ NIE	TAK/ NIE	TAK/ NIE

41 Środki zróżnicowane/ środki niezróżnicowane.

42 EFTA: Europejskie Stowarzyszenie Wolnego Handlu.

43 Kraje kandydujące oraz w stosownych przypadkach potencjalne kraje kandydujące Bałkanów Zachodnich.

3.2. Szacunkowy wpływ na wydatki

3.2.1. Synteza szacunkowego wpływu na wydatki

w mln EUR (do 3 miejsc po przecinku)

Dział wieloletnich ram finansowych:	1	Inteligentny i sprzyjający włączeniu społecznemu wzrost

Dyrekcja Generalna: <…….>			2015* [44]	Rok **2016**	Rok **2017**	Rok **2018**	Kolejne lata (2019-2021) i później			**OGÓŁEM**
• Środki operacyjne										
09 03 02	Środki na zobowiązania	(1)	1,250**	0,000						**1,250**
	Środki na płatności	(2)	0,750	0,250	0,250					**1,250**
Środki administracyjne finansowane ze środków przydzielonych na określone programy operacyjne[45]			**0,000**							**0,000**
Numer pozycji w budżecie		(3)	**0,000**							**0,000**
OGÓŁEM środki dla dyrekcji generalnej <….>	Środki na zobowiązania	=1+1a +3	1,250	0,000						**1,250**
	Środki na płatności	=2+2a +3	0,750	0,250	0,250					**1,250**

• OGÓŁEM środki operacyjne	Środki na zobowiązania	(4)	1,250	0,000						**1,250**

[44] Rok N jest rokiem, w którym rozpoczyna się wprowadzanie w życie wniosku/inicjatywy.

[45] Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie w zakresie wprowadzania w życie programów lub działań UE (dawne pozycje „BA"), pośrednie badania naukowe, bezpośrednie badania naukowe.

	Środki na płatności	(5)	0,750	0,250	0,250					**1,250**
• OGÓŁEM środki administracyjne finansowane ze środków przydzielonych na określone programy operacyjne		(6)	**0,000**							
OGÓŁEM środki na DZIAŁ 1 wieloletnich ram finansowych	Środki na zobowiązania	=4+ 6	1,250	0,000						**1,250**
	Środki na płatności	=5+ 6	0,750	0,250	0,250					**1,250**

* Dokładny termin będzie zależał od daty przyjęcia wniosku przez władzę ustawodawczą (tj. jeśli dyrektywa zostanie przyjęta w 2014 r., dostosowanie istniejącej infrastruktury rozpocznie się w 2015 r., w przeciwnym razie rok później).

** Jeżeli państwa członkowskie podejmą decyzję o wykorzystaniu istniejącej infrastruktury i pokryją jednorazowe koszty dostosowania w ramach budżetu UE, jak wyjaśniono w ppkt 1.4.3 i 1.7, koszt dostosowania sieci w celu umożliwienia współpracy między państwami członkowskimi, zgodnie z rozdziałem III dyrektywy (wczesne ostrzeżenia, skoordynowana reakcja itp.) szacuje się na 1 250 000 EUR. Kwota ta jest nieco wyższa niż kwota wymieniona w ocenie skutków („około 1 mln EUR"), ponieważ opiera się na bardziej dokładnym oszacowaniu kosztów niezbędnych elementów składających się na tego rodzaju infrastrukturę. Niezbędne elementy i związane z nimi koszty oparte są na szacunkach WCB, w oparciu o jego doświadczenia w zakresie opracowywania podobnych systemów stosowanych w innych dziedzinach, takich jak publiczna opieka zdrowotna, i obejmują: system szybkiego ostrzegania i zgłaszania w zakresie bezpieczeństwa sieci i informacji (275 000 EUR), platformę wymiany informacji (400 000 EUR), system wczesnego ostrzegania i reagowania (275 000 EUR) oraz centrum sytuacyjne (300 000 EUR), o łącznej wartości 1 250 000 EUR. Bardziej szczegółowy plan wdrożenia znajdzie się w oczekiwanym w najbliższej przyszłości studium wykonalności realizowanym na mocy umowy szczegółowej SMART 2012/0010: „Studium wykonalności i działania przygotowawcze na potrzeby wdrożenia europejskiego systemu wczesnego ostrzegania i reagowania przed atakami i zakłóceniami cybernetycznymi".

Jeżeli wpływ wniosku/inicjatywy nie ogranicza się do jednego działu:

• OGÓŁEM środki operacyjne	Środki na zobowiązania	(4)	0,000	0,000						
	Środki na płatności	(5)	0,000	0,000						
• OGÓŁEM środki administracyjne finansowane ze środków przydzielonych na określone programy operacyjne		(6)	**0,000**	**0,000**						
OGÓŁEM środki	Środki na zobowiązania	=4+ 6	1,250	0.000						1,250

na DZIAŁY 1 do 4 wieloletnich ram finansowych (kwota referencyjna)	Środki na płatności	=5+ 6	0,750	0,250	0,250					1,250

Dział wieloletnich ram finansowych	**5**	„Wydatki administracyjne”

w mln EUR (do 3 miejsc po przecinku)

		Rok **2015**	Rok **2016**	Rok **2017**	Rok **2018**	Kolejne lata (2019-2021) i później			**OGÓŁEM**
Dyrekcja Generalna: CNECT									
• Zasoby ludzkie		0,572	0,572	0,572	0,572	0,572	0,572	**0,572**	**4,004**
• Pozostałe wydatki administracyjne		0,318	0,118	0,318	0,118	0,318	0,118	**0,118**	**1,426**
OGÓŁEM DG CNECT	Środki	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

OGÓŁEM środki na DZIAŁ 5 wieloletnich ram finansowych	(Środki na zobowiązania ogółem = środki na płatności ogółem)	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

w mln EUR (do 3 miejsc po przecinku)

		Rok **2015**[46]	Rok **2016**	Rok **2017**	Rok **2018**	Kolejne lata (2019-2021) i później			**OGÓŁEM**
OGÓŁEM środki na DZIAŁY 1 do 5 wieloletnich ram finansowych	Środki na zobowiązania	2,140	0,690	0,890	0,690	0,890	0,690	0,690	**6,680**
	Środki na płatności	1,640	0,940	1,140	0,690	0,890	0,690	0,690	**6,680**

[46] Rok N jest rokiem, w którym rozpoczyna się wprowadzanie w życie wniosku/inicjatywy.

3.2.2. Szacunkowy wpływ na środki operacyjne

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków operacyjnych

– ☑ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków operacyjnych, jak określono poniżej:

– Środki na zobowiązania w mln EUR (do 3 miejsc po przecinku)

Określić cele i realizacje ⇩			Rok **2015***		Rok **2016**		Rok **2017**		Rok **2018**		Kolejne lata (2019-2021) i później						**OGÓŁEM**	
	REALIZACJA																	
	Rodzaj[47]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba całkowita	Koszt całkowity
CEL SZCZEGÓŁOWY nr 2[48] Infrastruktura do bezpiecznej wymiany informacji																		
Realizacja	Dostosowanie infrastruktury																	
Suma cząstkowa dla celu szczegółowego nr 2			1	1.250**													1	1.250
KOSZT OGÓŁEM				1.250														1.250

47 Realizacje odnoszą się do produktów i usług, które zostaną zapewnione (np.: liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

48 Zgodnie z opisem w punkcie 1.4.2. „Cel (cele) szczegółowy (-e)...".

* Dokładny termin będzie zależał od daty przyjęcia wniosku przez władzę ustawodawczą (tj. jeśli dyrektywa zostanie przyjęta w 2014 r., dostosowanie istniejącej infrastruktury rozpocznie się w 2015 r., w przeciwnym razie rok później).

** Zob. pkt 3.2.1

3.2.3. Szacunkowy wpływ na środki administracyjne

3.2.3.1. Streszczenie

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków administracyjnych

– ☑ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków administracyjnych, jak określono poniżej:

w mln EUR (do 3 miejsc po przecinku)

	Rok **2015**[49]	Rok **2016**	Rok **2017**	Rok **2018**	Kolejne lata (2019-2021) i później			**OGÓŁEM**
DZIAŁ 5 wieloletnich ram finansowych								
Zasoby ludzkie	0,572	0,572	0,572	0,572	0,572	0,572	0,572	**4,004**
Pozostałe wydatki administracyjne	0,318	0,118	0,318	0,118	0,318	0,118	0,118	**1,426**
Suma cząstkowa w DZIALE 5 wieloletnich ram finansowych	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
Poza DZIAŁEM 5[50] **wieloletnich ram finansowych**								
Zasoby ludzkie	0,000	0,000						**0,000**
Pozostałe wydatki administracyjne								
Suma cząstkowa poza DZIAŁEM 5 wieloletnich ram finansowych	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
OGÓŁEM	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Środki administracyjne zostaną pokryte ze środków DG CNECT już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach tej dyrekcji, uzupełnionych w razie potrzeby wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej

[49] Rok N jest rokiem, w którym rozpoczyna się wprowadzanie w życie wniosku/inicjatywy.

[50] Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie w zakresie wprowadzania w życie programów lub działań UE (dawne pozycje „BA"), pośrednie badania naukowe, bezpośrednie badania naukowe.

dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle ograniczeń budżetowych.

ENISA może wspomóc państwa członkowskie i Komisję w procesie wdrażania dyrektywy na podstawie udzielonego jej mandatu oraz poprzez przegrupowanie zasobów przewidzianych w ramach wieloletnich ram finansowych na okres 2014–2020 dla tej agencji, tzn. bez żadnych dodatkowych środków budżetowych lub zasobów ludzkich.

3.2.3.2. Szacowane zapotrzebowanie na zasoby ludzkie

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania zasobów ludzkich

– ☑ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania przez Komisję zasobów ludzkich, jak określono poniżej:

Zasadniczo nie będzie potrzebny dodatkowy personel. Potrzeby w zakresie zasobów ludzkich będą bardzo ograniczone i zostaną zaspokojone przez personel dyrekcji generalnej, który już teraz przydzielony jest do zarządzania działaniem.

Wartości szacunkowe należy wyrazić w pełnych kwotach (lub najwyżej z dokładnością do jednego miejsca po przecinku)

		Rok **2015**	Rok **2016**	Rok **2017**	Rok **2018**	Kolejne lata (2019-2021) i później		
• Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i pracowników zatrudnionych na czas określony)								
09 01 01 01 (w centrali i w biurach przedstawicielstw Komisji)		4	4	4	4	4	4	4
XX 01 01 02 (w delegaturach)								
XX 01 05 01 (pośrednie badania naukowe)								
10 01 05 01 (bezpośrednie badania naukowe)								
• Personel zewnętrzny (w ekwiwalentach pełnego czasu pracy)[51]								
09 01 02 01 (AC, END, INT z ogólnej puli środków finansowych)		1	1	1	1	1	1	1
XX 01 02 02 (AC, AL, END, INT i JED w delegaturach)								
XX 01 04 ***yy***[52]	w centrali[53]							
	w delegaturach							
XX 01 05 02 (AC, END, INT – pośrednie badania naukowe)								
10 01 05 02 (AC, END, INT – bezpośrednie badania naukowe)								
Inna pozycja w budżecie (określić)								
OGÓŁEM		**5**	**5**	**5**	**5**	**5**	**5**	**5**

XX oznacza odpowiednią dziedzinę polityki lub odpowiedni tytuł w budżecie.

Potrzeby w zakresie zasobów ludzkich zostaną pokryte z zasobów DG CNECT już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach dyrekcji generalnej, uzupełnionych w razie potrzeby

[51] AC= pracownik kontraktowy; INT= pracownik tymczasowy; JED= młodszy oddelegowany ekspert; AL = członek personelu miejscowego; END= oddelegowany ekspert krajowy.

[52] W ramach pułapu na personel zewnętrzny ze środków operacyjnych (dawne pozycje „BA").

[53] Przede wszystkim fundusze strukturalne, Europejski Fundusz Rolny na rzecz Rozwoju Obszarów Wiejskich (EFRROW) oraz Europejski Fundusz Rybacki.

wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle ograniczeń budżetowych.

ENISA może wspomóc państwa członkowskie i Komisję w procesie wdrażania dyrektywy na podstawie udzielonego jej mandatu oraz poprzez przegrupowanie zasobów przewidzianych w ramach wieloletnich ram finansowych na okres 2014–2020 dla tej agencji, tzn. bez żadnych dodatkowych środków budżetowych lub zasobów ludzkich.

Opis zadań do wykonania:

Urzędnicy i pracownicy zatrudnieni na czas określony	– Przygotowywanie aktów delegowanych zgodnie z art. 14 ust. 3 – Przygotowywanie aktów wykonawczych zgodnie z art. 8, art. 9 ust. 2, art. 12, art. 14 ust. 5, art. 16 – Wspieranie współpracy w ramach sieci zarówno na szczeblu politycznym, jak i operacyjnym – Udział w negocjacjach międzynarodowych i ewentualne zawieranie umów międzynarodowych
Personel zewnętrzny	Pomoc w realizacji powyższych zadań, jeżeli okaże się konieczna.

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

– ☑ Wniosek/inicjatywa jest zgodny(-a) z obowiązującymi wieloletnimi ramami finansowymi.

– ☐ Wniosek/inicjatywa wymaga przeprogramowania odpowiedniego działu w wieloletnich ramach finansowych.

Wniosek będzie miał szacowany wpływ finansowy na wydatki operacyjne, jeśli państwa członkowskie zdecydują się na dostosowanie istniejącej infrastruktury i powierzą Komisji zadanie wdrożenia tego dostosowania w ramach wieloletnich ram finansowych 2014–2020. Powiązane koszty jednorazowe zostałyby pokryte w ramach instrumentu „Łącząc Europę”, pod warunkiem że dostępne będą wystarczające środki. Alternatywnie państwa członkowskie mogą podzielić się kosztami dostosowania infrastruktury lub kosztami ustanowienia nowej infrastruktury.

– ☐ Wniosek/inicjatywa wymaga zastosowania instrumentu elastyczności lub zmiany wieloletnich ram finansowych[54]

Nie dotyczy.

3.2.5. Udział osób trzecich w finansowaniu

– Wniosek/inicjatywa nie przewiduje współfinansowania ze strony osób trzecich

3.3. Szacunkowy wpływ na dochody

– ☑ Wniosek/inicjatywa nie ma wpływu finansowego na dochody.

[54] Zob. pkt 19 i 24 porozumienia międzyinstytucjonalnego.