I

(Akty ustawodawcze)

DYREKTYWY

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/1148

z dnia 6 lipca 2016 r.

w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium 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]),

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([2]),

a także mając na uwadze, co następuje:

(1) Sieci oraz systemy i usługi informatyczne pełnią ważną rolę w społeczeństwie. Ich niezawodność i bezpieczeństwo mają zasadnicze znaczenie dla działalności gospodarczej i społecznej, w szczególności dla funkcjonowania rynku wewnętrznego.

(2) Skala, częstotliwość oraz wpływ incydentów w zakresie bezpieczeństwa stają się coraz większe i stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. Systemy te mogą się również stać obiektem umyślnych szkodliwych działań, mających na celu uszkodzenie lub przerwanie ich działania. Tego typu incydenty mogą utrudniać prowadzenie działalności gospodarczej, powodować znaczne straty finansowe, podważać zaufanie użytkowników oraz powodować poważne straty w gospodarce Unii.

(3) Sieci i systemy informatyczne, a przede wszystkim internet, odgrywają istotną rolę w ułatwianiu transgranicznego przepływu towarów, usług i osób. Ze względu na ponadnarodowy charakter tych systemów, ich znaczne zakłócenia – niezależnie od tego, czy umyślne czy nieumyślne, oraz niezależnie od tego, gdzie występują – mogą mieć wpływ zarówno na poszczególne państwa członkowskie, jak i na całą na Unię. Bezpieczeństwo sieci i systemów informatycznych ma zatem zasadnicze znaczenie dla sprawnego funkcjonowania rynku wewnętrznego.

(4) Kontynuując poczynione w ramach Europejskiego Forum Państw Członkowskich znaczące postępy w zakresie prowadzenia dyskusji i wymiany doświadczeń dotyczących dobrych praktyk w dziedzinie polityki, w tym opracowanie zasad europejskiej współpracy na wypadek kryzysów w cyberprzestrzeni, należy utworzyć grupę współpracy, złożoną z przedstawicieli państw członkowskich, Komisji oraz Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (zwanej dalej „ENISA") w celu wspierania i ułatwiania współpracy strategicznej między państwami członkowskimi w zakresie bezpieczeństwa sieci i systemów informatycznych. Aby grupa ta była

([1]) Dz.U. C 271 z 19.9.2013, s. 133.

([2]) Stanowisko Parlamentu Europejskiego z dnia 13 marca 2014 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz stanowisko Rady w pierwszym czytaniu z dnia 17 maja 2016 r. (dotychczas nieopublikowane w Dzienniku Urzędowym). Stanowisko Parlamentu Europejskiego z dnia 6 lipca 2016 r. (dotychczas nieopublikowane w Dzienniku Urzędowym).

skuteczna i dostępna dla wszystkich, konieczne jest, aby wszystkie państwa członkowskie posiadały minimalne zdolności i strategię zapewniające wysoki poziom bezpieczeństwa sieci i systemów informatycznych na ich terytorium. Ponadto wymogi dotyczące bezpieczeństwa i zgłaszania incydentów powinny mieć zastosowanie do operatorów usług kluczowych oraz do dostawców usług cyfrowych, aby propagować kulturę zarządzania ryzykiem i zapewnić zgłaszanie najpoważniejszych incydentów.

(5) Obecne zdolności nie są wystarczające do zapewnienia wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii. Państwa członkowskie bardzo się różnią pod względem poziomu gotowości, co powoduje niejednolite podejście w ramach Unii. Prowadzi to do nierównego poziomu ochrony konsumentów i przedsiębiorców oraz negatywnie wpływa na ogólny poziom bezpieczeństwa sieci i systemów informatycznych w Unii. Z kolei brak wspólnych wymogów dotyczących operatorów usług kluczowych i dostawców usług cyfrowych uniemożliwia ustanowienie całościowego i skutecznego mechanizmu współpracy na poziomie Unii. Uczelnie i ośrodki badań naukowych mają do odegrania zasadniczą rolę w pobudzaniu badań, rozwoju i innowacyjności w tych obszarach.

(6) Skuteczne reagowanie na wyzwania związane z zapewnieniem bezpieczeństwa sieci i systemów informatycznych wymaga zatem przyjęcia całościowego podejścia na poziomie Unii, obejmującego wymogi dotyczące budowania i planowania wspólnych minimalnych zdolności, wymianę informacji, współpracę oraz wspólne wymogi w zakresie bezpieczeństwa dla operatorów usług kluczowych i dostawców usług cyfrowych. Niemniej jednak operatorom usług kluczowych i dostawcom usług cyfrowych nie uniemożliwia się wdrażania bardziej rygorystycznych środków bezpieczeństwa niż te przewidziane w niniejszej dyrektywie.

(7) W celu uwzględnienia wszystkich istotnych incydentów i ryzyk niniejsza dyrektywa powinna mieć zastosowanie zarówno do operatorów usług kluczowych, jak i dostawców usług cyfrowych. Obowiązki nakładane na operatorów usług kluczowych i dostawców usług cyfrowych nie powinny jednak mieć zastosowania do przedsiębiorstw udostępniających publiczne sieci łączności lub świadczących publicznie dostępne usługi łączności elektronicznej w rozumieniu dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady ([1]), które podlegają szczegółowym wymogom w zakresie bezpieczeństwa i integralności ustanowionym w tej dyrektywie, ani nie powinny mieć zastosowania do dostawców usług zaufania w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 ([2]), którzy podlegają wymogom w zakresie bezpieczeństwa określonym w tym rozporządzeniu.

(8) Niniejsza dyrektywa pozostaje bez uszczerbku dla możliwości podjęcia przez każde z państw członkowskich środków niezbędnych do zapewnienia ochrony podstawowych interesów jego bezpieczeństwa, do ochrony porządku publicznego i bezpieczeństwa publicznego oraz do umożliwienia prowadzenia postępowań przygotowawczych, wykrywania i ścigania przestępstw. Zgodnie z art. 346 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) żadne państwo członkowskie nie ma obowiązku udzielania informacji, których ujawnienie uznaje za sprzeczne z podstawowymi interesami swojego bezpieczeństwa. W tym kontekście zastosowanie mają decyzja Rady 2013/488/UE ([3]) oraz umowy o nieujawnianiu lub nieformalne umowy o nieujawnianiu, takie jak reguły poufności TLP (Traffic Light Protocol).

(9) Niektóre sektory gospodarki są już regulowane lub mogą być w przyszłości regulowane sektorowymi aktami prawnymi Unii, które zawierają przepisy dotyczące bezpieczeństwa sieci i systemów informatycznych. W każdym przypadku gdy wspomniane akty prawne Unii zawierają przepisy nakładające wymogi dotyczące bezpieczeństwa sieci i systemów informatycznych lub zgłoszeń incydentów, przepisy te należy stosować, o ile zawierają wymogi, które są co najmniej równoważne pod względem skutku obowiązkom zawartym w niniejszej dyrektywie. Państwa członkowskie powinny zatem stosować przepisy takiego sektorowego aktu prawnego Unii, w tym przepisy odnoszące się do jurysdykcji, i nie powinny prowadzić procedury identyfikowania operatorów usług kluczowych zgodnie z definicją zawartą w niniejszej dyrektywie. W tym kontekście państwa członkowskie powinny przekazywać Komisji informacje dotyczące stosowania takich przepisów szczególnych. Przy ustalaniu, czy wymogi dotyczące bezpieczeństwa sieci i systemów informatycznych oraz zgłaszania incydentów zawarte w sektorowych aktach prawnych Unii są równoważne wymogom zawartym w niniejszej dyrektywie, należy uwzględniać wyłącznie przepisy odpowiednich aktów prawnych Unii i ich stosowanie w państwach członkowskich.

(10) W sektorze transportu wodnego wymogi w zakresie bezpieczeństwa dla przedsiębiorców, statków, obiektów portowych, portów i systemów ruchu statków obejmują zgodnie z aktami prawnymi Unii wszystkie działania, w tym również systemy radiowe i telekomunikacyjne, systemy komputerowe i sieci. Część obowiązkowych procedur postępowania obejmuje zgłaszanie wszystkich incydentów i powinna zatem być traktowana jako przepisy szczególne, o ile wymogi te są co najmniej równoważne z odpowiednimi przepisami niniejszej dyrektywy.

([1]) Dyrektywa 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) (Dz.U. L 108 z 24.4.2002, s. 33).

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U. L 257 z 28.8.2014, s. 73).

([3]) Decyzja Rady 2013/488/UE z dnia 23 września 2013 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz.U. L 274 z 15.10.2013, s. 1).

(11) Identyfikując operatorów w sektorze transportu wodnego, państwa członkowskie powinny – z myślą o zapewnieniu poszczególnym operatorom morskim spójnego podejścia – uwzględniać obecne i przyszłe międzynarodowe zasady i wytyczne opracowane w szczególności przez Międzynarodową Organizację Morską.

(12) Regulacje i nadzór w sektorach bankowości i infrastruktury rynków finansowych są w dużym stopniu zharmonizowane na poziomie Unii poprzez zastosowanie pierwotnego i wtórnego prawa Unii oraz norm opracowanych wspólnie z europejskimi organami nadzoru. W ramach unii bankowej stosowanie i nadzorowanie tych wymogów zapewniane jest przez jednolity mechanizm nadzorczy. W odniesieniu do państw członkowskich, które nie są częścią unii bankowej, zapewniane jest to przez odpowiednie bankowe organy regulacyjne państw członkowskich. W innych obszarach regulacji sektora finansowego Europejski System Nadzoru Finansowego również zapewnia wysoki stopień uspójnienia i konwergencji praktyk nadzorczych. Europejski Urząd Nadzoru Giełd i Papierów Wartościowych pełni również funkcję bezpośredniego nadzoru nad niektórymi podmiotami, a mianowicie agencjami ratingowymi i repozytoriami transakcji.

(13) Ryzyko operacyjne jest istotną częścią regulacji ostrożnościowej i nadzoru w sektorach bankowości i infrastruktury rynków finansowych. Obejmuje wszystkie operacje, w tym bezpieczeństwo, integralność i odporność sieci i systemów informatycznych. Wymogi w odniesieniu do tych systemów, które często wykraczają poza wymogi przewidziane w niniejszej dyrektywie, zawarte są w szeregu aktów prawnych Unii i obejmują: przepisy dotyczące warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi oraz przepisy dotyczące wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, w tym również wymogi dotyczące ryzyka operacyjnego; przepisy dotyczące rynków instrumentów finansowych, które obejmują wymogi dotyczące oceny ryzyka dla firm inwestycyjnych i rynków regulowanych; przepisy dotyczące instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji, które obejmują wymogi dotyczące ryzyka operacyjnego dla kontrahentów centralnych i repozytoriów transakcji; oraz przepisy dotyczące usprawnienia rozrachunku papierów wartościowych w Unii i dotyczące centralnych depozytów papierów wartościowych, które obejmują wymogi dotyczące ryzyka operacyjnego. Ponadto wymogi dotyczące zgłaszania incydentów są częścią normalnej praktyki nadzorczej w sektorze finansowym i są często włączane do podręczników dotyczących nadzoru. Państwa członkowskie powinny uwzględniać te przepisy i wymogi przy stosowaniu przepisów szczególnych.

(14) Jak zauważył Europejski Bank Centralny w swojej opinii z dnia 25 lipca 2014 r. ([1]), niniejsza dyrektywa nie wpływa na system regulujący w ramach prawa Unii nadzór Eurosystemu nad systemami płatności i rozrachunku. Organy odpowiedzialne za taki nadzór powinny wymieniać doświadczenia w sprawach dotyczących bezpieczeństwa sieci i systemów informatycznych z właściwymi organami w ramach niniejszej dyrektywy. To samo stosuje się do członków Europejskiego Systemu Banków Centralnych spoza strefy euro sprawujących taki nadzór nad systemami płatności i rozrachunku na podstawie krajowych przepisów ustawowych i wykonawczych.

(15) Internetowa platforma handlowa umożliwia konsumentom i przedsiębiorcom handlowym zawieranie umów sprzedaży lub umów o świadczenie usług online z przedsiębiorcami handlowymi i jest ostatecznym miejscem zawierania tych umów. W przypadku gdy możliwe jest ostateczne zawarcie umowy, nie powinna ona obejmować usług online, które spełniają wyłącznie funkcję pośredniczącą wobec usług stron trzecich. Nie powinna zatem obejmować usług online, które porównują cenę poszczególnych produktów lub usług różnych przedsiębiorców handlowych, a następnie przekierowują użytkownika do preferowanego przedsiębiorcy handlowego w celu zakupu produktu. Usługi komputerowe świadczone przez internetową platformę handlową mogą obejmować przetwarzanie transakcji, agregowanie danych lub profilowanie użytkowników. Sklepy z aplikacjami, które działają jako sklepy internetowe umożliwiające cyfrową dystrybucję aplikacji lub oprogramowania stron trzecich, należy traktować jako rodzaj internetowej platformy handlowej.

(16) Wyszukiwarka internetowa za pomocą zapytania na jakikolwiek temat umożliwia użytkownikowi wykonywanie przeszukań zasadniczo wszystkich stron internetowych. Alternatywnie wyszukiwanie może zostać zawężone do stron internetowych w konkretnym języku. Definicja wyszukiwarki internetowej zawarta w niniejszej dyrektywie nie powinna obejmować funkcji wyszukiwania, które ograniczają się do treści na konkretnej stronie internetowej, bez względu na to, czy funkcja wyszukiwania jest zapewniana przez wyszukiwarkę zewnętrzną. Nie powinna również obejmować usług online, które porównują cenę poszczególnych produktów lub usług różnych przedsiębiorców handlowych, a następnie przekierowują użytkownika do preferowanego przedsiębiorcy handlowego, aby tam dokonał zakupu produktu.

(17) Usługi przetwarzania w chmurze obejmują szeroki zakres działań, które mogą być realizowane według różnych modeli. Do celów niniejszej dyrektywy pojęcie „usługi przetwarzania w chmurze" obejmuje usługi, które umożliwiają dostęp do skalowalnego i elastycznego zbioru zasobów komputerowych do wspólnego wykorzystywania. Pojęcie „zasoby obliczeniowe" obejmuje zasoby takie, jak: sieci, serwery lub inną infrastrukturę, pamięć, aplikacje i usługi. Pojęcie „skalowalne" odnosi się do zasobów komputerowych, które są elastycznie przydzielane

([1]) Dz.U. C 352 z 7.10.2014, s. 4.

przez dostawcę usługi niezależnie od położenia geograficznego zasobów, jako reakcja na fluktuacje zapotrzebowania. Pojęcia „elastyczny zbiór" używa się do opisu tych zasobów obliczeniowych, które są przydzielane i uwalniane zależnie do zapotrzebowania, aby szybko zwiększać i zmniejszać dostępne zasoby w zależności od obciążenia. Pojęcia „wspólne wykorzystywanie" używa się do opisu zasobów obliczeniowych udostępnianych wielu użytkownikom, którzy dzielą wspólny dostęp do usługi, jednak przetwarzanie odbywa się oddzielnie dla każdego z użytkowników, choć usługa ta jest świadczona z tego samego sprzętu elektronicznego.

(18) Funkcją punktów wymiany ruchu internetowego (IXP) jest międzysystemowe łączenie sieci. IXP nie zapewnia dostępu do sieci ani nie działa jako realizator tranzytu czy operator infrastruktury tranzytu. IXP nie świadczy też innych usług niezwiązanych z połączeniem międzysystemowym, chociaż nie uniemożliwia to operatorowi IXP świadczenia także takich usług. IXP służy temu, aby łączyć ze sobą sieci, które są technicznie i organizacyjnie rozdzielone. Pojęcia „system autonomiczny" używa się do opisu sieci technicznie niezależnej.

(19) Państwa członkowskie powinny być odpowiedzialne za określanie, które podmioty spełniają kryteria definicji operatora usług kluczowych. Aby zapewnić spójne podejście, definicja operatora usług kluczowych powinna być stosowana w sposób spójny przez wszystkie państwa członkowskie. W tym celu niniejsza dyrektywa przewiduje: ocenę podmiotów działających w poszczególnych sektorach i podsektorach; sporządzenie wykazu usług kluczowych; rozpatrzenie wspólnego wykazu czynników międzysektorowych w celu ustalenia, czy ewentualny incydent mógłby mieć istotny skutek zakłócający; proces konsultacji z udziałem odnośnych państw członkowskich w przypadku podmiotów świadczących usługi w więcej niż jednym państwie członkowskim; a także wsparcie ze strony grupy współpracy w procesie identyfikacji operatorów. W celu zapewnienia, aby ewentualne zmiany na rynku były odpowiednio odzwierciedlane, państwa członkowskie powinny poddawać wykaz zidentyfikowanych operatorów regularnemu przeglądowi i w razie potrzeby go aktualizować. Ponadto państwa członkowskie powinny przekazywać Komisji informacje niezbędne do oceny, w jakim stopniu ta wspólna metodologia pozwoliła na spójne stosowanie definicji przez państwa członkowskie.

(20) W procesie identyfikowania operatorów usług kluczowych państwa członkowskie powinny dokonywać oceny – co najmniej w odniesieniu do każdego podsektora, o którym mowa w niniejszej dyrektywie – tego, które usługi muszą być uznane za kluczowe dla utrzymania krytycznej działalności społecznej i gospodarczej, oraz tego, czy podmioty zaliczone do sektorów i podsektorów, o których mowa w niniejszej dyrektywie, oraz świadczące te usługi, spełniają kryteria identyfikacji operatorów. Oceniając, czy podmiot świadczy usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wystarczy zbadać, czy podmiot ten świadczy usługę ujętą w wykazie usług kluczowych. Ponadto należy wykazać, że świadczenie usługi kluczowej zależy od sieci i systemów informatycznych. Poza tym przy ocenie, czy incydent mógłby mieć istotny zakłócający skutek dla świadczenia usługi, państwa członkowskie powinny uwzględnić szereg czynników międzysektorowych, a także, w stosownych przypadkach, czynniki sektorowe.

(21) Na potrzeby identyfikacji operatorów usług kluczowych posiadanie jednostki organizacyjnej w państwie członkowskim wiąże się z koniecznością prowadzenia działalności w sposób efektywny i rzeczywisty poprzez stabilne struktury. Forma prawna takich struktur, niezależnie od tego, czy chodzi o oddział czy podmiot zależny posiadający osobowość prawną, nie jest w tym względzie czynnikiem decydującym.

(22) Możliwe jest świadczenie przez podmioty działające w sektorach i podsektorach, o których mowa w niniejszej dyrektywie, zarówno usług kluczowych, jak i usług innych niż kluczowe. Na przykład w sektorze transportu lotniczego porty lotnicze świadczą usługi, które państwo członkowskie mogłoby uważać za kluczowe, takie jak zarządzanie drogami startowymi, ale również szereg usług, które mogłyby być uważane za usługi inne niż kluczowe, takie jak zapewnianie powierzchni handlowych. Operatorzy usług kluczowych powinni podlegać szczegółowym wymogom w zakresie bezpieczeństwa jedynie w odniesieniu do tych usług, które uznaje się za kluczowe. Na potrzeby identyfikacji operatorów państwa członkowskie powinny zatem ustanowić wykaz usług, które uważają za kluczowe.

(23) Wykaz usług powinien zawierać wszystkie usługi świadczone na terytorium danego państwa członkowskiego, które spełniają wymogi w ramach niniejszej dyrektywy. Państwa członkowskie powinny móc uzupełniać istniejący wykaz o nowe usługi. Wykaz usług powinien służyć jako punkt odniesienia dla państw członkowskich, umożliwiający identyfikację operatorów usług kluczowych. Jego celem jest identyfikacja rodzajów usług kluczowych w każdym z sektorów, o których mowa w niniejszej dyrektywie, co odróżniłoby je od działań innych niż kluczowe, za które podmiot działający w danym sektorze mógłby być odpowiedzialny. Wykaz usług ustanowiony przez każde z państw członkowskich stanowiłby dalszy wkład w ocenę praktyk regulacyjnych poszczególnych państw członkowskich z myślą o zapewnieniu ogólnego poziomu spójności procesu identyfikacji wśród państw członkowskich.

(24) Na potrzeby procesu identyfikacji, w przypadku gdy podmiot świadczy usługę kluczową w dwóch lub większej liczbie państw członkowskich, te państwa członkowskie powinny podjąć między sobą dwustronne lub wielostronne rozmowy. Ten proces konsultacji ma w zamierzeniu pomóc im w ocenie krytycznego charakteru danego operatora, jeżeli chodzi o wpływ transgraniczny, umożliwiając tym samym każdemu z zaangażowanych państw członkowskich przedstawienie swoich uwag dotyczących ryzyk związanych ze świadczonymi usługami. Zainteresowane państwa członkowskie powinny wzajemnie uwzględniać swoje poglądy w ramach tego procesu oraz powinny móc zwrócić się w tym zakresie o pomoc do grupy współpracy.

(25) W wyniku procesu identyfikacji państwa członkowskie powinny przyjąć środki krajowe w celu określenia, które podmioty podlegają obowiązkom dotyczącym bezpieczeństwa sieci i systemów informatycznych. Rezultat ten można by osiągnąć przez przyjęcie wykazu zawierającego wszystkich operatorów usług kluczowych lub przez przyjęcie środków krajowych zawierających obiektywne kryteria ilościowe, takie jak efekt końcowy działalności operatora lub liczba użytkowników, które umożliwiają określenie, które podmioty są objęte obowiązkami dotyczącymi bezpieczeństwa sieci i systemów informatycznych. Środki krajowe, już istniejące czy też przyjęte w kontekście niniejszej dyrektywy, powinny obejmować wszystkie środki prawne, środki administracyjne oraz polityki umożliwiające identyfikację operatorów usług kluczowych na mocy niniejszej dyrektywy.

(26) Aby określić w przybliżeniu znaczenie – w odniesieniu do danego sektora – zidentyfikowanych operatorów usług kluczowych, państwa członkowskie powinny wziąć pod uwagę liczbę i wielkość tych operatorów, na przykład pod względem udziału w rynku lub wolumenu produkcji lub transportu, bez obowiązku podawania informacji, które mogłyby ujawnić, którzy operatorzy zostali zidentyfikowani.

(27) W celu określenia, czy incydent mógłby mieć istotny skutek zakłócający dla świadczenia usługi kluczowej, państwa członkowskie powinny wziąć pod uwagę szereg różnych czynników, takich jak liczba użytkowników zależnych od korzystania z tej usługi do celów prywatnych lub zawodowych. Korzystanie z tej usługi może mieć charakter bezpośredni, niebezpośredni lub odbywać się za pomocą pośrednictwa. Oceniając wpływ, jaki incydent ten mógłby mieć, pod względem skali i czasu trwania, na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne, państwa członkowskie powinny również oszacować czas, jaki może upłynąć, zanim przerwanie usługi zaczęłoby wywierać negatywny wpływ.

(28) Aby określić, czy incydent mógłby mieć istotny skutek zakłócający dla świadczenia usługi kluczowej, oprócz czynników międzysektorowych należy uwzględnić także czynniki sektorowe. W odniesieniu do dostawców energii takie czynniki mogłyby obejmować wielkość lub udział w krajowej produkcji energii; w odniesieniu do dostawców ropy naftowej – dzienną wielkość dostaw; w odniesieniu do transportu lotniczego, w tym portów lotniczych i przewoźników lotniczych, transportu kolejowego i portów morskich – udział w wolumenie ruchu krajowego i roczną liczbę pasażerów lub przewozów towarowych; w odniesieniu do bankowości lub infrastruktury rynków finansowych – ich znaczenie systemowe na podstawie sumy aktywów lub stosunek tej sumy aktywów do PKB; w odniesieniu do sektora ochrony zdrowia – roczną liczbę pacjentów objętych opieką usługodawcy; w odniesieniu do produkcji, uzdatniania i dostaw wody – jej ilości, a także liczbę i rodzaje zaopatrywanych użytkowników – w tym na przykład szpitale, służba publiczna, organizacje lub osoby indywidualne – oraz istnienie alternatywnych źródeł wody na tym samym obszarze geograficznym.

(29) Aby osiągnąć i utrzymać wysoki poziom bezpieczeństwa sieci i systemów informatycznych, każde państwo członkowskie powinno posiadać krajową strategię w zakresie bezpieczeństwa sieci i systemów informatycznych określającą cele strategiczne i konkretne działania z zakresu polityki, które należy wdrożyć.

(30) Z uwagi na różnice w krajowych strukturach zarządzania oraz w celu zabezpieczenia obowiązujących już ustaleń sektorowych lub unijnych organów nadzorczych i regulacyjnych, a także w celu unikania powielania, państwa członkowskie powinny móc wyznaczać więcej niż jeden właściwy organ krajowy odpowiedzialny za wykonywanie zadań związanych z bezpieczeństwem sieci i systemów informatycznych operatorów usług kluczowych i dostawców usług cyfrowych na mocy niniejszej dyrektywy.

(31) W celu ułatwienia współpracy i komunikacji transgranicznej oraz umożliwienia skutecznego wprowadzenia w życie niniejszej dyrektywy, niezbędne jest, aby każde państwo członkowskie, bez uszczerbku dla sektorowych ustaleń regulacyjnych, wyznaczyło krajowy pojedynczy punkt kontaktowy odpowiedzialny za koordynację kwestii związanych z bezpieczeństwem sieci i systemów informatycznych oraz współpracę transgraniczną na poziomie Unii. Właściwym organom i pojedynczym punktom kontaktowym należy zapewnić wystarczające zasoby techniczne, finansowe i ludzkie, aby mogły skutecznie i efektywnie wykonywać powierzone im zadania i osiągnąć w ten sposób cele niniejszej dyrektywy. Ponieważ niniejsza dyrektywa ma na celu poprawę funkcjonowania rynku wewnętrznego poprzez budowanie zaufania i pewności, organy państw członkowskich muszą być w stanie skutecznie współpracować z podmiotami gospodarczymi i posiadać odpowiednią strukturę.

(32) Właściwe organy lub zespoły reagowania na incydenty bezpieczeństwa komputerowego (zwane dalej „CSIRT") powinny odbierać zgłoszenia incydentów. Pojedyncze punkty kontaktowe nie powinny bezpośrednio odbierać żadnych zgłoszeń incydentów, chyba że działają również jako właściwy organ lub CSIRT. Właściwy organ lub CSIRT powinny jednak móc zlecić pojedynczemu punktowi kontaktowemu przekazywanie zgłoszeń incydentów pojedynczym punktom kontaktowym innych państw członkowskich, których incydent dotyczy.

(33) Aby zapewnić efektywne przekazywanie informacji państwom członkowskim i Komisji, pojedynczy punkt kontaktowy powinien przedkładać grupie współpracy sprawozdania podsumowujące, które powinny być zanonimizowane w celu zachowania poufności zgłoszeń oraz tożsamości operatorów usług kluczowych i dostawców usług cyfrowych, ponieważ informacje dotyczące tożsamości zgłaszających podmiotów nie są wymagane do wymiany najlepszych praktyk w grupie współpracy. Sprawozdanie podsumowujące powinno zawierać informacje na temat liczby otrzymanych zgłoszeń, a także informacje o charakterze zgłoszonych incydentów, takie jak rodzaje naruszeń bezpieczeństwa, ich kluczowość lub czas ich trwania.

(34) Państwa członkowskie powinny zostać odpowiednio wyposażone, zarówno pod względem zdolności technicznych, jak i możliwości organizacyjnych, w celu zapobiegania incydentom i ryzykom dotyczącym sieci i systemów informatycznych, wykrywania ich, reagowania na nie i łagodzenia ich skutków. Państwa członkowskie powinny zatem zapewnić dobrze funkcjonujące CSIRT, zwane również zespołami reagowania na incydenty komputerowe (zwane dalej „CERT"), które spełniają zasadnicze wymogi w celu zagwarantowania efektywnych i kompatybilnych zdolności w zakresie postępowania z incydentami i ryzykami oraz zapewnienia skutecznej współpracy na poziomie Unii. Aby wszystkie rodzaje operatorów usług kluczowych i dostawców usług cyfrowych korzystały z tych zdolności i współpracy, państwa członkowskie powinny zapewnić, aby wszystkie rodzaje obejmował wyznaczony CSIRT. Z uwagi na znaczenie współpracy międzynarodowej w dziedzinie cyberbezpieczeństwa CSIRT powinny mieć możliwość uczestniczenia w międzynarodowych sieciach współpracy, niezależnie od współpracy w ramach sieci CSIRT ustanowionej na mocy niniejszej dyrektywy.

(35) Ponieważ większość sieci i systemów informatycznych eksploatowana jest przez podmioty prywatne, niezbędna jest współpraca między sektorem publicznym a sektorem prywatnym. Operatorów usług kluczowych i dostawców usług cyfrowych należy zachęcać do tworzenia własnych nieformalnych mechanizmów współpracy w celu zapewniania bezpieczeństwa sieci i systemów informatycznych. Grupa współpracy powinna móc, w stosownych przypadkach, zapraszać odpowiednie zainteresowane strony do dyskusji. W celu skutecznego zachęcania do dzielenia się informacjami oraz najlepszymi praktykami konieczne jest zapewnienie, aby operatorzy usług kluczowych i dostawcy usług cyfrowych uczestniczący w takich wymianach nie ponosili konsekwencji wynikających z samego faktu współpracy.

(36) ENISA powinna wspierać państwa członkowskie i Komisję przez udostępnianie wiedzy specjalistycznej i doradztwo oraz przez ułatwianie wymiany najlepszych praktyk. W szczególności przy stosowaniu niniejszej dyrektywy Komisja powinna konsultować się z ENISA, a państwa członkowskie powinny móc konsultować się z ENISA. Aby budować zdolności i wiedzę wśród państw członkowskich, grupa współpracy powinna również służyć jako narzędzie wymiany najlepszych praktyk, dyskusji na temat zdolności i gotowości państw członkowskich oraz – na zasadzie dobrowolności – aby pomóc jej członkom w ocenie krajowych strategii w zakresie bezpieczeństwa sieci i systemów informatycznych, w budowaniu potencjału i ocenie ćwiczeń z zakresu bezpieczeństwa sieci i systemów informatycznych.

(37) W stosownych przypadkach państwa członkowskie powinny mieć możliwość wykorzystania lub dostosowania istniejących struktur organizacyjnych lub strategii przy stosowaniu niniejszej dyrektywy.

(38) Odpowiednie zadania grupy współpracy i ENISA są współzależne i uzupełniają się. ENISA powinna na ogół wspomagać grupę współpracy w wykonywaniu jej zadań, zgodnie z celem ENISA określonym w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 526/2013 ([1]), a mianowicie w celu pomagania instytucjom, organom, urzędom i agencjom Unii oraz państwom członkowskim w realizacji polityki niezbędnej do spełniania wymogów prawnych i regulacyjnych w zakresie bezpieczeństwa sieci i systemów informatycznych określonych w obowiązujących i przyszłych aktach prawnych Unii. W szczególności ENISA powinna udzielać pomocy w tych dziedzinach, które odpowiadają jej własnym zadaniom, określonym w rozporządzeniu (UE) nr 526/2013, a mianowicie w zakresie analizy strategii w zakresie bezpieczeństwa sieci i systemów informatycznych, wspierania organizacji i prowadzenia unijnych ćwiczeń z zakresu bezpieczeństwa sieci i systemów informatycznych oraz wymiany informacji i najlepszych praktyk w zakresie podnoszenia świadomości i szkoleń. ENISA powinna być także włączona w opracowywanie wytycznych dotyczących sektorowych kryteriów określania istotności wpływu incydentu.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r. w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004 (Dz.U. L 165 z 18.6.2013, s. 41).

(39) W celu propagowania zaawansowanych systemów bezpieczeństwa sieci i systemów informatycznych grupa współpracy powinna, w stosownych przypadkach, współpracować z odpowiednimi instytucjami, organami, urzędami i agencjami Unii, aby wymieniać się wiedzą i najlepszymi praktykami oraz doradzać w sprawie aspektów bezpieczeństwa sieci i systemów informatycznych, które mogłyby mieć wpływ na ich pracę, przestrzegając jednocześnie istniejących ustaleń w zakresie wymiany informacji zastrzeżonych. Współpracując z organami ścigania w kwestiach dotyczących bezpieczeństwa sieci i systemów informatycznych, które mogłyby mieć wpływ na jej pracę, grupa współpracy powinna uwzględniać istniejące kanały informacji i ustanowione sieci.

(40) Informacje na temat incydentów są coraz cenniejsze dla ogółu społeczeństwa i przedsiębiorstw, w szczególności dla małych i średnich przedsiębiorstw. W niektórych przypadkach takie informacje, skoncentrowane głównie na incydentach i wydarzeniach o wymiarze krajowym, są już dostępne za pośrednictwem stron internetowych na poziomie krajowym w języku danego kraju. W związku z tym, że przedsiębiorstwa w coraz większym stopniu działają transgranicznie, a obywatele korzystają z usług online, informacje dotyczące incydentów powinny być przekazywane w formie zagregowanej na poziomie Unii. Zachęca się sekretariat sieci CSIRT do prowadzenia strony internetowej lub wskazania specjalnej podstrony na istniejącej stronie internetowej, koncentrującej się szczególnie na interesach i potrzebach przedsiębiorców, gdzie ogólne informacje dotyczące poważnych incydentów na terytorium Unii byłyby udostępnione ogółowi społeczeństwa. Zachęca się CSIRT uczestniczące w sieci CSIRT do przekazywania na zasadzie dobrowolności informacji do celów publikowania na tej stronie internetowej, niezawierających informacji poufnych lub szczególnie chronionych.

(41) W przypadku gdy informacje uznaje się za poufne zgodnie z unijnymi i krajowymi przepisami dotyczącymi tajemnicy przedsiębiorstwa, w trakcie wykonywania czynności i realizacji celów określonych w niniejszej dyrektywie należy zapewnić taką poufność.

(42) Dla sprawdzenia gotowości i współpracy państw członkowskich w odniesieniu do bezpieczeństwa sieci i systemów informatycznych istotne znaczenie mają ćwiczenia w zakresie cyberbezpieczeństwa, które symulują scenariusze incydentów w czasie rzeczywistym. Cykl ćwiczeń CyberEurope koordynowany przez ENISA z udziałem państw członkowskich stanowi użyteczne narzędzie do takiego sprawdzenia i opracowywania zaleceń dotyczących tego, jak z czasem należy usprawniać sposoby postępowania w przypadku incydentu na poziomie Unii. Zważywszy, że państwa członkowskie nie są obecnie objęte jakimkolwiek obowiązkiem planowania ćwiczeń lub brania w nich udziału, utworzenie sieci CSIRT na mocy niniejszej dyrektywy powinno umożliwić państwom członkowskim udział w ćwiczeniach w oparciu o odpowiednie wybory w zakresie planowania i strategii. Grupa współpracy ustanowiona na mocy niniejszej dyrektywy powinna prowadzić dyskusje na temat strategicznych decyzji dotyczących ćwiczeń, w szczególności – lecz nie wyłącznie – w zakresie regularności ćwiczeń i opracowywania scenariuszy. ENISA powinna zgodnie ze swoim mandatem wspierać organizację i prowadzenie ogólnounijnych ćwiczeń przez udostępnienie swojej wiedzy specjalistycznej i doradztwa grupie współpracy i sieci CSIRT.

(43) Ze względu na globalny charakter problemów związanych z bezpieczeństwem sieci i systemów informatycznych istnieje potrzeba zacieśnienia współpracy międzynarodowej w celu poprawy norm bezpieczeństwa i wymiany informacji oraz w celu propagowania wspólnego całościowego podejścia do kwestii bezpieczeństwa.

(44) Odpowiedzialność za zapewnienie bezpieczeństwa sieci i systemów informatycznych w dużym stopniu spoczywa na operatorach usług kluczowych i dostawcach usług cyfrowych. Za pomocą odpowiednich wymogów regulacyjnych i dobrowolnych praktyk branżowych należy wspierać i rozwijać kulturę zarządzania ryzykiem, obejmującą przeprowadzanie ocen ryzyka i wdrażanie środków bezpieczeństwa odpowiednich dla danego ryzyka. Stworzenie wiarygodnych równych warunków działania ma również kluczowe znaczenie dla skutecznego funkcjonowania grupy współpracy i sieci CSIRT, w celu zapewnienia skutecznej współpracy ze strony wszystkich państw członkowskich.

(45) Niniejsza dyrektywa ma zastosowanie wyłącznie do tych administracji publicznych, które zostały zidentyfikowane jako operatorzy usług kluczowych. Państwa członkowskie pozostają jednak odpowiedzialne za zapewnienie bezpieczeństwa sieci i systemów informatycznych administracji publicznych niewchodzących w zakres stosowania niniejszej dyrektywy.

(46) Środki w zakresie zarządzania ryzykiem obejmują środki mające na celu identyfikację wszelkich ryzyk incydentów, zapobieganie incydentom, wykrywanie ich i postępowanie z nimi, a także łagodzenie ich wpływu. Bezpieczeństwo sieci i systemów informatycznych obejmuje bezpieczeństwo danych przechowywanych, przekazywanych i przetwarzanych.

(47) Właściwe organy powinny zachować możliwość przyjmowania krajowych wytycznych dotyczących okoliczności, w których operatorzy usług kluczowych są zobowiązani do zgłaszania incydentów.

(48) Wielu przedsiębiorców w Unii na potrzeby świadczenia swoich usług jest zależnych od dostawców usług cyfrowych. Ponieważ niektóre usługi cyfrowe mogłyby być ważnym zasobem dla ich użytkowników, w tym dla operatorów usług kluczowych, a użytkownicy ci nie zawsze mogą mieć dostępne alternatywy, niniejsza dyrektywa powinna mieć także zastosowanie do dostawców takich usług. Bezpieczeństwo, ciągłość i wiarygodność rodzaju usług cyfrowych, o którym mowa w niniejszej dyrektywie, mają istotne znaczenie dla sprawnego funkcjonowania wielu przedsiębiorców. Zakłócenie takich usług cyfrowych mogłoby uniemożliwić świadczenie innych usług, które są od nich zależne, i mogłoby w związku z tym mieć wpływ na kluczową działalność gospodarczą i społeczną w Unii. Takie usługi cyfrowe mogłyby mieć zatem kluczowe znaczenie dla sprawnego funkcjonowania przedsiębiorców zależnych od tych usług, a także dla uczestnictwa takich przedsiębiorców w rynku wewnętrznym i handlu transgranicznym w Unii. Za dostawców usług cyfrowych podlegających niniejszej dyrektywie uważa się dostawców oferujących usługi cyfrowe, od których zależnych jest w coraz większym stopniu wielu przedsiębiorców w Unii.

(49) Dostawcy usług cyfrowych powinni zapewnić poziom bezpieczeństwa współmierny do stopnia ryzyka, na jakie narażone jest bezpieczeństwo świadczonych przez nich usług cyfrowych, ze względu na znaczenie tych usług dla działalności innych przedsiębiorców w Unii. W praktyce stopień ryzyka dla operatorów usług kluczowych – które są często istotne dla utrzymania krytycznej działalności społecznej i gospodarczej – jest wyższy niż dla dostawców usług cyfrowych. Wymogi w zakresie bezpieczeństwa dotyczące dostawców usług cyfrowych powinny być zatem mniejsze. Dostawcom usług cyfrowych należy pozostawić swobodę podejmowania środków, które uznają za odpowiednie do zarządzania ryzykami, na jakie może być narażone bezpieczeństwo ich sieci i systemów informatycznych. Z powodu transgranicznego charakteru usług cyfrowych ich dostawcy powinni podlegać bardziej zharmonizowanemu podejściu na poziomie Unii. Akty wykonawcze powinny ułatwić uszczegółowienie i wdrażanie takich środków.

(50) Mimo iż producenci sprzętu i twórcy oprogramowania nie są operatorami usług kluczowych ani dostawcami usług cyfrowych, ich produkty zwiększają bezpieczeństwo sieci i systemów informatycznych. Odgrywają oni zatem ważną rolę w umożliwianiu operatorom usług kluczowych i dostawcom usług cyfrowych zabezpieczenia ich sieci i systemów informatycznych. Taki sprzęt i oprogramowanie są już objęte obowiązującymi przepisami dotyczącymi odpowiedzialności za produkt.

(51) Środki techniczne i organizacyjne nakładane na operatorów usług kluczowych i dostawców usług cyfrowych nie powinny wiązać się z koniecznością projektowania, opracowywania lub produkowania w określony sposób określonego produktu technologii teleinformatycznych dostępnego w handlu.

(52) Operatorzy usług kluczowych i dostawcy usług cyfrowych powinni zapewniać bezpieczeństwo sieci i systemów informatycznych, których używają. Dotyczy to przede wszystkim prywatnych sieci i systemów informatycznych, które są zarządzane przez własny personel informatyczny lub dla których zapewnienie bezpieczeństwa zlecono na zewnątrz. Wymogi w zakresie bezpieczeństwa i zgłaszania incydentów powinny mieć zastosowanie do odpowiednich operatorów usług kluczowych i dostawców usług cyfrowych bez względu na to, czy sami zapewniają obsługę swoich sieci i systemów informatycznych, czy też zlecają tę obsługę innym podmiotom.

(53) Aby uniknąć nakładania nieproporcjonalnie dużych obciążeń finansowych i administracyjnych na operatorów usług kluczowych i dostawców usług cyfrowych, wymogi powinny być proporcjonalne do ryzyka związanego z daną siecią oraz danym systemem informatycznym oraz powinny uwzględniać najnowszy stan wiedzy na temat takich środków. W przypadku dostawców usług cyfrowych wymogi te nie powinny mieć zastosowania do mikroprzedsiębiorstw ani małych przedsiębiorstw.

(54) W przypadku gdy administracje publiczne państw członkowskich korzystają z usług oferowanych przez dostawców usług cyfrowych, w szczególności usług przetwarzania w chmurze, mogłyby one wymagać od dostawców takich usług dodatkowych środków bezpieczeństwa oprócz tych, które normalnie oferowaliby dostawcy usług cyfrowych zgodnie z wymogami niniejszej dyrektywy. Powinny one mieć możliwość określenia takich wymogów w drodze zobowiązań umownych.

(55) Definicje internetowych platform handlowych, wyszukiwarek internetowych i usług przetwarzania w chmurze zawarte w niniejszej dyrektywie stosuje się specjalnie na potrzeby niniejszej dyrektywy oraz bez uszczerbku dla jakichkolwiek innych instrumentów.

(56) Niniejsza dyrektywa nie powinna uniemożliwiać państwom członkowskim przyjmowania środków krajowych zobowiązujących podmioty sektora publicznego do zapewnienia szczególnych wymogów w zakresie bezpieczeństwa, w przypadku gdy zawierają one umowy na usługi przetwarzania w chmurze. Takie środki krajowe powinny mieć zastosowanie do danego podmiotu sektora publicznego, a nie do dostawcy usług przetwarzania w chmurze.

(57) Biorąc pod uwagę podstawowe różnice między operatorami usług kluczowych, w szczególności ich bezpośredni związek z infrastrukturą fizyczną, a dostawcami usług cyfrowych, w szczególności ich transgraniczny charakter, należy przyjąć w niniejszej dyrektywie zróżnicowane podejście do poziomu harmonizacji względem tych dwóch grup podmiotów. W odniesieniu do usług kluczowych państwa członkowskie powinny móc identyfikować odpowiednich operatorów i nakładać wymogi bardziej rygorystyczne od tych określonych w niniejszej dyrektywie. Państwa członkowskie nie powinny identyfikować dostawców usług cyfrowych, ponieważ niniejsza dyrektywa powinna mieć zastosowanie do wszystkich dostawców usług cyfrowych objętych jej zakresem stosowania. Ponadto niniejsza dyrektywa oraz akty wykonawcze przyjęte na jej podstawie powinny zapewniać wysoki poziom harmonizacji względem dostawców usług cyfrowych w odniesieniu do wymogów w zakresie bezpieczeństwa i zgłaszania incydentów. Powinno to umożliwić jednolite traktowanie dostawców usług cyfrowych na terytorium Unii w sposób proporcjonalny do ich charakteru i stopnia ryzyka, z którym mogliby się zetknąć.

(58) Niniejsza dyrektywa nie powinna uniemożliwiać państwom członkowskim nakładania wymogów w zakresie bezpieczeństwa i zgłaszania incydentów na podmioty niebędące dostawcami usług cyfrowych objętymi zakresem stosowania niniejszej dyrektywy, bez uszczerbku dla obowiązków państw członkowskich wynikających z prawa Unii.

(59) Właściwe organy powinny zwracać należytą uwagę na zabezpieczenie nieformalnych i zaufanych kanałów wymiany informacji. Decyzje o informowaniu społeczeństwa o incydentach zgłoszonych właściwym organom należy podejmować przy zachowaniu należytej równowagi między interesem publicznym, zgodnie z którym społeczeństwo powinno być informowane o zagrożeniach, a ryzykiem utraty reputacji i poniesienia szkód handlowych, na jakie narażeni są operatorzy usług kluczowych i dostawcy usług cyfrowych zgłaszający incydenty. Wykonując obowiązki w zakresie zgłaszania incydentów, właściwe organy i CSIRT powinny zwracać szczególną uwagę na potrzebę zachowania ścisłej poufności w odniesieniu do informacji dotyczących podatności produktów, do czasu udostępnienia odpowiednich poprawek w zakresie bezpieczeństwa.

(60) Dostawcy usług cyfrowych powinni podlegać łagodnym i reaktywnym działaniom nadzorczym *ex post*, uzasadnionym przez charakter ich usług i działań. Zainteresowany właściwy organ powinien zatem podejmować działania wyłącznie wtedy, gdy otrzymał dowód – na przykład od samego dostawcy usług cyfrowych, innego właściwego organu, w tym właściwego organu innego państwa członkowskiego, lub od użytkownika usługi – że dostawca usług cyfrowych nie spełnia wymogów niniejszej dyrektywy, w szczególności w wyniku wystąpienia incydentu. Właściwy organ nie powinien zatem mieć ogólnego obowiązku nadzorowania dostawców usług cyfrowych.

(61) Właściwe organy powinny mieć środki niezbędne do wykonywania swoich obowiązków, w tym uprawnienia do uzyskiwania informacji wystarczających do oceny poziomu bezpieczeństwa sieci i systemów informatycznych.

(62) Incydenty mogą być wynikiem przestępstw, w odniesieniu do których zapobieganie, prowadzenie postępowania przygotowawczego i ściganie jest wspierane przez koordynację i współpracę między operatorami usług kluczowych, dostawcami usług cyfrowych, właściwymi organami i organami ścigania. W razie podejrzenia, że incydent ma związek z poważnymi przestępstwami w rozumieniu prawa Unii lub prawa krajowego, państwa członkowskie powinny zachęcać operatorów usług kluczowych i dostawców usług cyfrowych, aby zgłaszali odpowiednim organom ścigania incydenty noszące znamiona poważnego przestępstwa. W stosownych przypadkach pożądane jest, aby koordynacja między właściwymi organami a organami ścigania z różnych państw członkowskich była ułatwiana dzięki Europejskiemu Centrum ds. Walki z Cyberprzestępczością (EC3) oraz dzięki ENISA.

(63) W wielu przypadkach istnieje niebezpieczeństwo naruszenia danych osobowych w wyniku incydentów. W tym kontekście właściwe organy oraz organy ochrony danych powinny ze sobą współpracować oraz wymieniać się informacjami dotyczącymi wszystkich istotnych kwestii w celu rozwiązywania problemów związanych z wszelkimi przypadkami naruszeń danych osobowych w wyniku incydentów.

(64) Jurysdykcję w odniesieniu do dostawców usług cyfrowych należy powierzyć tylko jednemu państwu członkowskiemu, w którym dany dostawca usług cyfrowych ma główną jednostkę organizacyjną w Unii, co z zasady odpowiada miejscu, gdzie dostawca usług ma siedzibę zarządu w Unii. Pojęcie „jednostka organizacyjna" zakłada skuteczne i faktyczne prowadzenie działalności poprzez stabilne struktury. Forma prawna takich struktur,

niezależnie od tego, czy chodzi o oddział czy podmiot zależny posiadający osobowość prawną, nie jest w tym względzie czynnikiem decydującym. Kryterium to nie powinno zależeć od tego, czy sieć i systemy informatyczne są fizycznie zlokalizowane w danym miejscu; fizyczne położenie i wykorzystanie takich systemów nie stanowią same w sobie takiej głównej jednostki organizacyjnej i nie są zatem kryteriami określania głównej jednostki organizacyjnej.

(65) W przypadku gdy dostawca usług cyfrowych nieposiadający jednostki organizacyjnej w Unii oferuje usługi w Unii, dostawca taki powinien wyznaczyć przedstawiciela. Aby stwierdzić, czy dostawca usług cyfrowych oferuje usługi w Unii, należy upewnić się, czy jest oczywiste, że dany dostawca usług cyfrowych zamierza oferować usługi osobom w jednym lub większej liczbie państw członkowskich. Do ustalenia takiego zamiaru nie wystarczy sama dostępność w Unii strony internetowej dostawcy usług cyfrowych lub pośrednika lub adresu poczty elektronicznej i innych danych kontaktowych ani posługiwanie się językiem powszechnie stosowanym w państwie trzecim, w którym dostawca usług cyfrowych posiada jednostkę organizacyjną. Jednakże czynniki takie, jak posługiwanie się językiem lub walutą powszechnie stosowanymi w jednym lub większej liczbie państw członkowskich oraz możliwość zamówienia usług w tym języku lub wzmianka o klientach lub użytkownikach znajdujących się w Unii, mogą potwierdzać oczywistość zamiaru oferowania przez dostawcę usług cyfrowych usług w Unii. Przedstawiciel powinien występować w imieniu dostawcy usług cyfrowych, a właściwe organy lub CSIRT powinny móc kontaktować się z przedstawicielem. Przedstawiciel powinien zostać wyznaczony w sposób wyraźny za pomocą pisemnego upoważnienia dostawcy usług cyfrowych do występowania w jego imieniu w zakresie jego obowiązków wynikających z niniejszej dyrektywy, w tym zgłaszania incydentów.

(66) Normalizacja wymogów w zakresie bezpieczeństwa jest procesem napędzanym przez rynek. W celu zapewnienia zbieżnego stosowania norm bezpieczeństwa państwa członkowskie powinny zachęcać do zgodności lub zbieżności z określonymi normami w celu zapewnienia wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych na poziomie Unii. ENISA powinna pomagać państwom członkowskim za pomocą porad i wytycznych. W tym celu pomocne mogłoby być opracowanie zharmonizowanych norm, czego należy dokonać zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1025/2012 ([1]).

(67) Podmioty nieobjęte zakresem stosowania niniejszej dyrektywy mogą mieć do czynienia z incydentami mającymi istotny wpływ na usługi, które są przez nie świadczone. W przypadku gdy podmioty te uznają, że w interesie publicznym leży zgłoszenie wystąpienia takich incydentów, powinny mieć taką możliwość na zasadzie dobrowolności. Zgłoszenia te powinny być rozpatrywane przez właściwy organ lub CSIRT, w przypadku gdy ich rozpatrywanie nie stanowi nieproporcjonalnego czy nadmiernego obciążenia dla danych państw członkowskich.

(68) W celu zapewnienia jednolitych warunków wykonywania niniejszej dyrektywy należy powierzyć Komisji uprawnienia wykonawcze w celu określenia procedur niezbędnych do funkcjonowania grupy współpracy oraz wymogów dotyczących bezpieczeństwa i zgłaszania incydentów mających zastosowanie do dostawców usług cyfrowych. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 ([2]). Przyjmując akty wykonawcze dotyczące procedur niezbędnych do funkcjonowania grupy współpracy, Komisja powinna w jak największym stopniu uwzględnić opinię ENISA.

(69) Przyjmując akty wykonawcze dotyczące wymogów w zakresie bezpieczeństwa i zgłaszania incydentów w odniesieniu do dostawców usług cyfrowych, Komisja powinna w jak największym stopniu uwzględnić opinię ENISA oraz konsultować się z zainteresowanymi stronami. Ponadto zachęca się Komisję, aby uwzględniała następujące zagadnienia: w odniesieniu do bezpieczeństwa systemów i obiektów – bezpieczeństwo fizyczne i środowiskowe, bezpieczeństwo dostaw, kontrolę dostępu do sieci i systemów informatycznych oraz integralność sieci i systemów informatycznych; w odniesieniu do postępowania w przypadku incydentu – procedury postępowania w przypadku incydentu, zdolności wykrywania incydentów, zgłaszanie incydentów i informowanie o nich; w odniesieniu do zarządzania ciągłością działalności – strategię ciągłości usług i plany awaryjne, zdolności w zakresie przywracania gotowości do pracy po katastrofie; oraz w odniesieniu do monitorowania, prowadzenia audytu i testowania – polityki monitorowania i prowadzenia dzienników systemowych, ćwiczenia w zakresie planów awaryjnych, testowanie sieci i systemów informatycznych, oceny bezpieczeństwa i monitorowanie zgodności.

(70) Przy wykonywaniu niniejszej dyrektywy Komisja powinna w stosownych przypadkach współpracować z odpowiednimi komitetami sektorowymi oraz odpowiednimi podmiotami ustanowionymi na poziomie Unii w dziedzinie objętej zakresem stosowania niniejszej dyrektywy.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz.U. L 316 z 14.11.2012, s. 12).

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13).

(71) Komisja powinna okresowo dokonywać przeglądu niniejszej dyrektywy, w drodze konsultacji z zainteresowanymi stronami, w szczególności w celu sprawdzenia, czy konieczne jest wprowadzenie zmian w świetle zmieniających się warunków społecznych, politycznych, technologicznych lub rynkowych.

(72) Wymiana informacji dotyczących ryzyk i incydentów w ramach grupy współpracy i sieci CSIRT oraz zapewnienie zgodności z wymogami w zakresie zgłaszania incydentów właściwym organom krajowym lub CSIRT mogłyby oznaczać konieczność przetwarzania danych osobowych. Takie przetwarzanie powinno być zgodne z dyrektywą 95/46/WE Parlamentu Europejskiego i Rady ([1]) i rozporządzeniem (WE) nr 45/2001 Parlamentu Europejskiego i Rady ([2]). Przy stosowaniu niniejszej dyrektywy zastosowanie powinno mieć, w stosownych przypadkach, rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady ([3]).

(73) Zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 14 czerwca 2013 r. ([4]).

(74) Ponieważ cel niniejszej dyrektywy, a mianowicie osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast ze względu na skutki działania możliwe jest lepsze jego osiągnięcie na poziomie Unii, Unia może podjąć działania zgodnie z zasadą pomocniczości określoną 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.

(75) Niniejsza dyrektywa nie narusza praw podstawowych i jest zgodna z zasadami uznanymi w Karcie praw podstawowych Unii Europejskiej, w szczególności z 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 wprowadzać w życie zgodnie z tymi prawami i zasadami,

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot i zakres stosowania

1. Niniejsza dyrektywa ustanawia środki mające na celu osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii, aby poprawić funkcjonowanie rynku wewnętrznego.

2. W tym celu niniejsza dyrektywa:

a) ustanawia obowiązki dla wszystkich państw członkowskich dotyczące przyjęcia krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych;

b) tworzy grupę współpracy, aby wspierać i ułatwiać strategiczną współpracę i wymianę informacji między państwami członkowskimi oraz rozwijać wśród nich zaufanie i pewność;

c) tworzy sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (zwaną dalej „siecią CSIRT"), aby przyczyniać się do rozwijania zaufania i pewności między państwami członkowskimi oraz promować szybką i skuteczną współpracę operacyjną;

([1]) Dyrektywa 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 (Dz.U. L 281 z 23.11.1995, s. 31).

([2]) Rozporządzenie (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 (Dz.U. L 8 z 12.1.2001, s. 1).

([3]) 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 (Dz.U. L 145 z 31.5.2001, s. 43).

([4]) Dz.U. C 32 z 4.2.2014, s. 19.

d) ustanawia wymogi dotyczące bezpieczeństwa i zgłaszania incydentów dla operatorów usług kluczowych i dostawców usług cyfrowych;

e) ustanawia obowiązki dla państw członkowskich dotyczące wyznaczania właściwych organów krajowych, pojedynczych punktów kontaktowych oraz CSIRT mających zadania związane z bezpieczeństwem sieci i systemów informatycznych.

3. Wymogi dotyczące bezpieczeństwa i zgłaszania incydentów przewidziane w niniejszej dyrektywie nie mają zastosowania do przedsiębiorstw, które podlegają wymogom art. 13a i 13b dyrektywy 2002/21/WE, ani do dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia (UE) nr 910/2014.

4. Niniejszą dyrektywę stosuje się bez uszczerbku dla dyrektywy Rady 2008/114/WE ([1]) i dyrektyw Parlamentu Europejskiego i Rady 2011/93/UE ([2]) oraz 2013/40/UE ([3]).

5. Bez uszczerbku dla art. 346 TFUE informacje, które są poufne zgodnie z przepisami unijnymi i krajowymi, takimi jak przepisy dotyczące tajemnicy przedsiębiorstwa, podlegają wymianie z Komisją i innymi odpowiednimi organami tylko wtedy, gdy wymiana taka jest niezbędna do stosowania niniejszej dyrektywy. Informacje podlegające wymianie ogranicza się do tego, co jest istotne dla celów takiej wymiany i proporcjonalne do jej celów. Taka wymiana informacji musi zachować poufność tych informacji oraz chronić bezpieczeństwo i interesy handlowe operatorów usług kluczowych i dostawców usług cyfrowych.

6. Niniejsza dyrektywa pozostaje bez uszczerbku dla działań podejmowanych przez państwa członkowskie w celu zagwarantowania ich podstawowych funkcji państwowych, w szczególności w celu ochrony bezpieczeństwa narodowego – w tym działań na rzecz ochrony informacji, których ujawnienie państwa członkowskie uważają za sprzeczne z podstawowymi interesami swojego bezpieczeństwa – oraz w celu utrzymania porządku publicznego, w szczególności w celu umożliwienia prowadzenia postępowań przygotowawczych w sprawie przestępstw, ich wykrywania i ścigania.

7. W przypadku gdy sektorowy akt prawny Unii wymaga od operatorów usług kluczowych lub dostawców usług cyfrowych, aby zapewniali bezpieczeństwo swoich sieci i systemów informatycznych albo zgłaszali incydenty, stosuje się przepisy tego sektorowego aktu prawnego Unii, pod warunkiem że takie wymogi są przynajmniej równoważne pod względem skutku z obowiązkami określonymi w niniejszej dyrektywie.

Artykuł 2

Przetwarzanie danych osobowych

1. Przetwarzanie danych osobowych na mocy niniejszej dyrektywy odbywa się zgodnie z dyrektywą 95/46/WE.

2. Przetwarzanie danych osobowych przez instytucje i organy Unii na mocy niniejszej dyrektywy odbywa się zgodnie z rozporządzeniem (WE) nr 45/2001.

Artykuł 3

Harmonizacja minimalna

Państwa członkowskie mogą, bez uszczerbku dla art. 16 ust. 10 oraz dla ich obowiązków wynikających z prawa Unii, przyjmować lub utrzymywać przepisy mające na celu osiągnięcie wyższego poziomu bezpieczeństwa sieci i systemów informatycznych.

([1]) Dyrektywa 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 (Dz.U. L 345 z 23.12.2008, s. 75).

([2]) Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.U. L 335 z 17.12.2011, s. 1).

([3]) Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.U. L 218 z 14.8.2013, s. 8).

Artykuł 4

Definicje

Na potrzeby niniejszej dyrektywy stosuje się następujące definicje:

1) „sieci i systemy informatyczne" oznaczają:

   a) sieci łączności elektronicznej w rozumieniu art. 2 lit. a) dyrektywy 2002/21/WE;

   b) wszelkie urządzenia lub grupy wzajemnie połączonych lub powiązanych urządzeń, z których jedno lub większa ich liczba, wykonując program, dokonuje automatycznego przetwarzania danych cyfrowych; lub

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

2) „bezpieczeństwo sieci i systemów informatycznych" oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne;

3) „krajowa strategia w zakresie bezpieczeństwa sieci i systemów informatycznych" oznacza ramy zapewniające strategiczne cele i priorytety w zakresie bezpieczeństwa sieci i systemów informatycznych na poziomie krajowym;

4) „operator usług kluczowych" oznacza podmiot publiczny lub prywatny, należący do jednego z rodzajów, o których mowa w załączniku II, spełniający kryteria określone w art. 5 ust. 2;

5) „usługa cyfrowa" oznacza usługę w rozumieniu art. 1 ust. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535 ([1]), która należy do jednego z rodzajów wymienionych w załączniku III;

6) „dostawca usług cyfrowych" oznacza każdą osobę prawną, która świadczy usługi cyfrowe;

7) „incydent" oznacza każde zdarzenie, które ma rzeczywiście niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych;

8) „postępowanie w przypadku incydentu" oznacza wszystkie procedury umożliwiające wykrywanie i analizowanie incydentu, ograniczenie jego skutków oraz reagowanie na niego;

9) „ryzyko" oznacza każdą dającą się racjonalnie określić okoliczność lub zdarzenie, które ma potencjalny niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych;

10) „przedstawiciel" oznacza każdą osobę fizyczną lub prawną ustanowioną w Unii, wyraźnie wyznaczoną do występowania w imieniu dostawcy usług cyfrowych nieposiadającego jednostki organizacyjnej w Unii, do którego właściwy organ krajowy lub CSIRT może się zwrócić zamiast do dostawcy usług cyfrowych, w związku z obowiązkami dostawcy usług cyfrowych w ramach niniejszej dyrektywy;

11) „norma" oznacza normę w rozumieniu art. 2 pkt 1 rozporządzenia (UE) nr 1025/2012;

12) „specyfikacja" oznacza specyfikację techniczną w rozumieniu art. 2 pkt 4 rozporządzenia (UE) nr 1025/2012;

13) „punkt wymiany ruchu internetowego (IXP)" oznacza obiekt sieciowy, który umożliwia połączenie międzysystemowe pomiędzy więcej niż dwoma niezależnymi systemami autonomicznymi, głównie do celów ułatwienia wymiany ruchu internetowego; IXP zapewnia połączenie międzysystemowe wyłącznie systemów autonomicznych; IXP nie wymaga, aby ruch internetowy między jakąkolwiek parą uczestniczących systemów autonomicznych przechodził przez jakikolwiek trzeci system autonomiczny, ani nie powoduje zmian w tym ruchu, ani w inny sposób w niego nie ingeruje;

14) „system nazw domen (DNS)" oznacza hierarchiczny rozproszony system nazw sieciowych, który odpowiada na zapytania o nazwy domen;

([1]) Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.U. L 241 z 17.9.2015, s. 1).

15) „dostawca usług DNS" oznacza podmiot, która świadczy w internecie usługi DNS;

16) „rejestr nazw domen najwyższego poziomu" oznacza podmiot, który zarządza rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu (TLD) i dokonuje takiej rejestracji;

17) „internetowa platforma handlowa" oznacza usługę cyfrową, która umożliwia konsumentom lub przedsiębiorcom zdefiniowanym odpowiednio w art. 4 ust. 1 lit. a) i lit. b) dyrektywy Parlamentu Europejskiego i Rady 2013/11/UE ([1]) zawieranie online umów dotyczących sprzedaży lub usług z przedsiębiorcami na stronie internetowej platformy handlowej albo na stronie internetowej przedsiębiorcy, który używa usług komputerowych świadczonych przez internetową platformę handlową;

18) „wyszukiwarka internetowa" oznacza usługę cyfrową, która umożliwia użytkownikom wyszukiwanie – co do zasady – wszystkich stron internetowych lub stron internetowych w danym języku za pomocą zapytania na jakikolwiek temat przez podanie słowa kluczowego, wyrażenia lub innej wartości wejściowej; w wyniku przedstawia ona odnośniki, pod którymi można znaleźć informacje związane z zadanym zapytaniem;

19) „usługa przetwarzania w chmurze" oznacza usługę cyfrową umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania.

Artykuł 5

Identyfikacja operatorów usług kluczowych

1. W terminie do dnia 9 listopada 2018 r. w odniesieniu do każdego sektora i podsektora, o których mowa w załączniku II, państwa członkowskie identyfikują operatorów usług kluczowych posiadających jednostkę organizacyjną na ich terytorium.

2. Kryteria identyfikacji operatorów usług kluczowych, o których mowa w art. 4 pkt 4, są następujące:

a) podmiot świadczy usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej;

b) świadczenie tej usługi zależy od sieci i systemów informatycznych; oraz

c) incydent miałby istotny skutek zakłócający dla świadczenia tej usługi.

3. Do celów ust. 1 każde państwo członkowskie ustanawia wykaz usług, o których mowa w ust. 2 lit. a).

4. Do celów ust. 1, w przypadku gdy podmiot świadczy usługę, o której mowa w ust. 2 lit. a), w dwóch lub większej liczbie państw członkowskich, te państwa członkowskie wzajemnie się konsultują. Konsultacje te odbywają się przed podjęciem decyzji o identyfikacji.

5. Państwa członkowskie regularnie, lecz nie rzadziej niż co dwa lata, po dniu 9 maja 2018 r., dokonują przeglądu oraz, w stosownych przypadkach, aktualizują wykaz zidentyfikowanych operatorów usług kluczowych.

6. Rolą grupy współpracy jest, zgodnie z zadaniami, o których mowa w art. 11, wspieranie państw członkowskich w przyjmowaniu spójnego podejścia w procesie identyfikacji operatorów usług kluczowych.

7. Do celów przeglądu, o którym mowa w art. 23, oraz w terminie do dnia 9 listopada 2018 r., a następnie co dwa lata, państwa członkowskie przekazują Komisji niezbędne informacje, aby umożliwić jej ocenę wdrażania niniejszej dyrektywy, w szczególności spójności podejść państw członkowskich w zakresie identyfikacji operatorów usług kluczowych. Informacje te obejmują co najmniej:

a) krajowe środki umożliwiające identyfikowanie operatorów usług kluczowych;

([1]) Dyrektywa Parlamentu Europejskiego i Rady 2013/11/UE z dnia 21 maja 2013 r. w sprawie alternatywnych metod rozstrzygania sporów konsumenckich oraz zmiany rozporządzenia (WE) nr 2006/2004 i dyrektywy 2009/22/WE (dyrektywa w sprawie ADR w sporach konsumenckich) (Dz.U. L 165 z 18.6.2013, s. 63).

b) wykaz usług, o którym mowa w ust. 3;

c) liczbę zidentyfikowanych operatorów usług kluczowych w każdym z sektorów, o których mowa w załączniku II, oraz wskazanie ich znaczenia w odniesieniu do tego sektora;

d) progi, jeżeli istnieją, w celu określenia odpowiedniego poziomu dostaw w powiązaniu z liczbą użytkowników zależnych od tej usługi zgodnie z art. 6 ust. 1 lit. a) lub znaczenia tego konkretnego operatora usług kluczowych zgodnie z art. 6 ust. 1 lit. f).

Aby przyczynić się do dostarczania porównywalnych informacji, Komisja – w jak największym stopniu uwzględniając opinię ENISA – może przyjąć odpowiednie wytyczne techniczne dotyczące parametrów w odniesieniu do informacji, o których mowa w niniejszym ustępie.

Artykuł 6

Istotny skutek zakłócający

1. Przy określaniu istotności skutku zakłócającego, o którym mowa w art. 5 ust. 2 lit. c), państwa członkowskie uwzględniają co najmniej następujące czynniki międzysektorowe:

a) liczbę użytkowników zależnych od usługi świadczonej przez dany podmiot;

b) zależność innych sektorów, o których mowa w załączniku II, od usługi świadczonej przez ten podmiot;

c) wpływ, jaki incydenty – jeżeli chodzi o ich skalę i czas trwania – mogłyby mieć na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne;

d) udział tego podmiotu w rynku;

e) zasięg geograficzny związany z obszarem, którego mógłby dotyczyć incydent;

f) znaczenie podmiotu w utrzymywaniu wystarczającego poziomu usługi przy uwzględnieniu dostępności alternatywnych sposobów świadczenia tej usługi.

2. W celu ustalenia, czy incydent miałby istotny skutek zakłócający, państwa członkowskie, w stosownych przypadkach, uwzględniają także czynniki sektorowe.

ROZDZIAŁ II

RAMY KRAJOWE W ZAKRESIE BEZPIECZEŃSTWA SIECI I SYSTEMÓW INFORMATYCZNYCH

Artykuł 7

Krajowa strategia w zakresie bezpieczeństwa sieci i systemów informatycznych

1. Każde państwo członkowskie przyjmuje krajową strategię w zakresie bezpieczeństwa sieci i systemów informatycznych określającą cele strategiczne i odpowiednie środki polityczne i regulacyjne mające na celu osiągnięcie i utrzymanie wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych oraz obejmujące co najmniej sektory, o których mowa w załączniku II, i usługi, o których mowa w załączniku III. Krajowa strategia w zakresie bezpieczeństwa sieci i systemów informatycznych uwzględnia w szczególności następujące kwestie:

a) cele i priorytety krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych;

b) ramy zarządzania służące realizacji celów i priorytetów krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych, w tym role i zakresy obowiązków organów rządowych i innych właściwych podmiotów;

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

d) wskazówki odnoszące się do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących do strategii w zakresie bezpieczeństwa sieci i systemów informatycznych;

e) wskazówki odnoszące się do planów badawczo-rozwojowych dotyczących strategii w zakresie bezpieczeństwa sieci i systemów informatycznych;

f) plan oceny ryzyka służący określeniu ryzyk;

g) wykaz różnych podmiotów zaangażowanych we wdrażanie strategii w zakresie bezpieczeństwa sieci i systemów informatycznych.

2. Państwa członkowskie mogą zwrócić się do ENISA o pomoc przy opracowywaniu krajowych strategii w zakresie bezpieczeństwa sieci i systemów informatycznych.

3. Państwa członkowskie przekazują Komisji swoje krajowe strategie w zakresie bezpieczeństwa sieci i systemów informatycznych w ciągu trzech miesięcy od ich przyjęcia. Przekazując te strategie, państwa członkowskie mogą wyłączyć elementy strategii, które są związane z bezpieczeństwem narodowym.

Artykuł 8

Właściwe organy krajowe i pojedynczy punkt kontaktowy

1. Każde państwo członkowskie wyznacza jeden lub większą liczbę właściwych organów krajowych ds. bezpieczeństwa sieci i systemów informatycznych (zwanych dalej „właściwym organem"), obejmujących co najmniej sektory, o których mowa w załączniku II, i usługi, o których mowa w załączniku III. Państwa członkowskie mogą do tej roli wyznaczyć istniejący organ lub istniejące organy.

2. Właściwe organy monitorują stosowanie niniejszej dyrektywy na poziomie krajowym.

3. Każde państwo członkowskie wyznacza krajowy pojedynczy punkt kontaktowy ds. bezpieczeństwa sieci i systemów informatycznych (zwany dalej „pojedynczym punktem kontaktowym"). Państwa członkowskie mogą do tej roli wyznaczyć istniejący organ. W przypadku gdy państwo członkowskie wyznacza tylko jeden właściwy organ, ten właściwy organ jest również pojedynczym punktem kontaktowym.

4. Pojedynczy punkt kontaktowy pełni funkcję łącznikową w celu zapewnienia transgranicznej współpracy organów państw członkowskich oraz współpracy z odpowiednimi organami w innych państwach członkowskich, a także z grupą współpracy, o której mowa w art. 11, i siecią CSIRT, o której mowa w art. 12.

5. Państwa członkowskie zapewniają właściwym organom i pojedynczym punktom kontaktowym odpowiednie zasoby, aby mogły one efektywnie i skutecznie wykonywać powierzone im zadania z myślą o osiągnięciu celów niniejszej dyrektywy. Państwa członkowskie zapewniają efektywną, skuteczną i bezpieczną współpracę wyznaczonych przedstawicieli w grupie współpracy.

6. Właściwe organy i pojedynczy punkt kontaktowy, w stosownych przypadkach oraz zgodnie z prawem krajowym, konsultują się i współpracują z odpowiednimi krajowymi organami ścigania i krajowymi organami ochrony danych.

7. Każde państwo członkowskie niezwłocznie powiadamia Komisję o wyznaczeniu właściwego organu i pojedynczego punktu kontaktowego, o ich zadaniach i o wszelkich późniejszych zmianach w tym zakresie. Każde państwo członkowskie podaje do publicznej wiadomości informację o wyznaczeniu właściwego organu i pojedynczego punktu kontaktowego. Komisja publikuje wykaz wyznaczonych pojedynczych punktów kontaktowych.

Artykuł 9

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT)

1. Każde państwo członkowskie wyznacza jeden lub większą liczbę CSIRT spełniających wymogi zawarte w załączniku I pkt 1, obejmujących przynajmniej sektory, o których mowa w załączniku II, i usługi, o których mowa w załączniku III, odpowiedzialnych za postępowanie w odniesieniu do ryzyk i postępowanie w przypadku incydentu zgodnie z jasno określoną procedurą. CSIRT mogą być ustanawiane w ramach właściwego organu.

2. Państwa członkowskie zapewniają, aby CSIRT miały odpowiednie zasoby w celu skutecznej realizacji swoich zadań określonych w załączniku I pkt 2.

Państwa członkowskie zapewniają skuteczną, efektywną i bezpieczną współpracę swoich CSIRT w ramach sieci CSIRT, o której mowa w art. 12.

3. Państwa członkowskie zapewniają, aby ich CSIRT miały dostęp do odpowiedniej, bezpiecznej i odpornej infrastruktury komunikacyjno-informacyjnej na poziomie krajowym.

4. Państwa członkowskie przekazują Komisji informacje o zakresie kompetencji CSIRT, jak również o głównych elementach procedur postępowania w przypadku incydentu.

5. Państwa członkowskie mogą zwrócić się do ENISA o pomoc przy tworzeniu krajowych CSIRT.

Artykuł 10

Współpraca na poziomie krajowym

1. W przypadku gdy właściwy organ, pojedynczy punkt kontaktowy i CSIRT tego samego państwa członkowskiego są oddzielne, współpracują ze sobą w zakresie wypełnienia obowiązków określonych w niniejszej dyrektywie.

2. Państwa członkowskie zapewniają, aby właściwe organy albo CSIRT odbierały zgłoszenia o incydentach przekazane na mocy niniejszej dyrektywy. W przypadku gdy państwo członkowskie postanowi, że CSIRT nie będą odbierać zgłoszeń, CSIRT otrzymają, w stopniu koniecznym do wykonywania swoich zadań, dostęp do danych dotyczących incydentów zgłaszanych przez operatorów usług kluczowych na mocy art. 14 ust. 3 i 5 lub przez dostawców usług cyfrowych na mocy art. 16 ust. 3 i 6.

3. Państwa członkowskie zapewniają, aby właściwe organy lub CSIRT informowały pojedyncze punkty kontaktowe o zgłoszeniach incydentów przekazanych na mocy niniejszej dyrektywy.

W terminie do dnia 9 sierpnia 2018 r., a następnie raz do roku pojedynczy punkt kontaktowy przekazuje grupie współpracy sprawozdanie podsumowujące na temat otrzymanych zgłoszeń, w tym liczby zgłoszeń i charakteru zgłoszonych incydentów, oraz działań podjętych zgodnie z art. 14 ust. 3 i 5 oraz art. 16 ust. 3 i 6.

ROZDZIAŁ III

WSPÓŁPRACA

Artykuł 11

Grupa współpracy

1. Niniejszym ustanawia się grupę współpracy, aby wesprzeć i ułatwić strategiczną współpracę i wymianę informacji między państwami członkowskimi oraz wzmocnić zaufanie i pewność, a także z myślą o osiągnięciu wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii.

Grupa współpracy wykonuje swoje zadania na podstawie dwuletnich programów prac, o których mowa w ust. 3 akapit drugi.

2. Grupa współpracy składa się z przedstawicieli państw członkowskich, Komisji i ENISA.

W stosownych przypadkach grupa współpracy może zaprosić przedstawicieli odpowiednich zainteresowanych stron do udziału w swoich pracach.

Komisja zapewnia sekretariat.

3. Zadania grupy współpracy są następujące:

a) udzielanie strategicznych wskazówek dotyczących działalności sieci CSIRT ustanowionej na mocy art. 12;

b) wymiana najlepszych praktyk dotyczących wymiany informacji związanej ze zgłaszaniem incydentów, o którym mowa w art. 14 ust. 3 i 5 i art. 16 ust. 3 i 6;

c) wymiana najlepszych praktyk między państwami członkowskimi oraz, we współpracy z ENISA, pomoc państwom członkowskim w budowaniu zdolności z myślą o zapewnieniu bezpieczeństwa sieci i systemów informatycznych;

d) omawianie zdolności i gotowości państw członkowskich oraz, na zasadzie dobrowolności, ocena krajowych strategii w zakresie bezpieczeństwa sieci i systemów informatycznych oraz skuteczności CSIRT, a także określanie najlepszych praktyk;

e) wymiana informacji i najlepszych praktyk dotyczących podnoszenia świadomości i szkolenia;

f) wymiana informacji i najlepszych praktyk dotyczących badań i rozwoju w zakresie bezpieczeństwa sieci i systemów informatycznych;

g) w stosownych przypadkach, wymiana doświadczeń w sprawach dotyczących bezpieczeństwa sieci i systemów informatycznych z odpowiednimi instytucjami, organami, biurami i agencjami Unii;

h) omawianie z przedstawicielami odpowiednich europejskich organizacji normalizacyjnych norm i specyfikacji, o których mowa w art. 19;

i) gromadzenie informacji z zakresu najlepszych praktyk dotyczących ryzyk i incydentów;

j) coroczna analiza sprawozdań podsumowujących, o których mowa w art. 10 ust. 3 akapit drugi;

k) omawianie prac podjętych w odniesieniu do ćwiczeń dotyczących bezpieczeństwa sieci i systemów informatycznych, programów edukacyjnych i szkoleń, w tym prac wykonywanych przez ENISA;

l) przy wsparciu ENISA – wymiana najlepszych praktyk w odniesieniu do identyfikowania operatorów usług kluczowych przez państwa członkowskie, w tym w odniesieniu do transgranicznych zależności, dotyczących ryzyk i incydentów;

m) omawianie zasad dotyczących sprawozdawczości w zakresie zgłaszania incydentów, o których mowa w art. 14 i 16.

W terminie do dnia 9 lutego 2018 r., a następnie co dwa lata grupa współpracy opracowuje program prac w odniesieniu do działań, jakie mają zostać podjęte w celu realizacji celów i zadań, które muszą być spójne z celami niniejszej dyrektywy.

4. Na potrzeby przeglądu, o którym mowa w art. 23, w terminie do dnia 9 sierpnia 2018 r., a następnie co półtora roku grupa współpracy przygotowuje sprawozdanie oceniające doświadczenia zdobyte w ramach strategicznej współpracy prowadzonej na mocy niniejszego artykułu.

5. Komisja przyjmuje akty wykonawcze określające procedury niezbędne do funkcjonowania grupy współpracy. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 22 ust. 2.

Do celów akapitu pierwszego Komisja przedkłada pierwszy projekt aktu wykonawczego komitetowi, o którym mowa w art. 22 ust. 1, w terminie do dnia 9 lutego 2017 r.

Artykuł 12

Sieć CSIRT

1. Niniejszym ustanawia się sieć krajowych CSIRT w celu przyczyniania się do rozwoju pewności i zaufania między państwami członkowskimi oraz propagowania szybkiej i skutecznej współpracy.

2. Sieć CSIRT składa się z przedstawicieli CSIRT państw członkowskich i CERT-EU. Komisja uczestniczy w sieci CSIRT jako obserwator. ENISA zapewnia sekretariat oraz aktywnie wspiera współpracę między CSIRT.

3. Zadania sieci CSIRT są następujące:

a) wymiana informacji dotyczących usług, operacji i zdolności współpracy CSIRT;

b) na wniosek przedstawiciela CSIRT z państwa członkowskiego, na które potencjalnie może mieć wpływ incydent – wymiana i dyskusja dotycząca informacji innych niż szczególnie chronione informacje handlowe, związanych z tym incydentem i powiązanymi ryzykami; jednakże CSIRT każdego z państw członkowskich może odmówić wkładu w tę dyskusję, jeżeli istnieje ryzyko szkody dla postępowania przygotowawczego w sprawie incydentu;

c) wymiana i udostępnienie na zasadzie dobrowolności informacji innych niż poufne, dotyczących poszczególnych incydentów;

d) na wniosek przedstawiciela państwa członkowskiego – omówienie oraz, w miarę możliwości, określenie skoordynowanej reakcji na incydent, który został zidentyfikowany w ramach jurysdykcji tego państwa członkowskiego;

e) zapewnianie wsparcia państw członkowskich w obsłudze incydentów transgranicznych w oparciu o ich dobrowolną wzajemną pomoc;

f) omówienie, zbadanie i określenie dalszych form współpracy operacyjnej, w tym w związku z:

   (i) kategoriami ryzyk i incydentów;

   (ii) wczesnym ostrzeganiem;

   (iii) wzajemną pomocą;

   (iv) zasadami i uzgodnieniami dotyczącymi koordynacji, gdy państwa członkowskie reagują na transgraniczne ryzyka i incydenty;

g) informowanie grupy współpracy o swoich działaniach i o dalszych formach współpracy operacyjnej omawianych zgodnie z lit. f) oraz zwracanie się o wskazówki w tym zakresie;

h) omawianie wniosków z ćwiczeń dotyczących bezpieczeństwa sieci i systemów informatycznych, w tym ćwiczeń organizowanych przez ENISA;

i) na wniosek danego CSIRT – omawianie zdolności i gotowości tego CSIRT;

j) wydawanie wytycznych w celu ułatwienia konwergencji praktyk operacyjnych w odniesieniu do stosowania przepisów niniejszego artykułu dotyczących współpracy operacyjnej.

4. Na potrzeby przeglądu, o którym mowa w art. 23, w terminie do dnia 9 sierpnia 2018 r., a następnie co półtora roku, sieć CSRIT przedstawia sprawozdanie zawierające ocenę doświadczeń zdobytych w ramach współpracy operacyjnej, wraz z wnioskami i zaleceniami, prowadzonej na mocy niniejszego artykułu. Sprawozdanie to jest także przedkładane grupie współpracy.

5. Sieć CSIRT ustanawia swój regulamin wewnętrzny.

Artykuł 13

Współpraca międzynarodowa

Unia może zawierać umowy międzynarodowe, zgodnie z art. 218 TFUE, z państwami trzecimi lub organizacjami międzynarodowymi, umożliwiając i organizując ich udział w niektórych działaniach grupy współpracy. Takie umowy muszą uwzględniać potrzebę zapewnienia odpowiedniej ochrony danych.

ROZDZIAŁ IV

BEZPIECZEŃSTWO SIECI I SYSTEMÓW INFORMATYCZNYCH OPERATORÓW USŁUG KLUCZOWYCH

Artykuł 14

Wymogi w zakresie bezpieczeństwa i zgłaszanie incydentów

1. Państwa członkowskie zapewniają, aby operatorzy usług kluczowych podejmowali odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykami, na jakie narażone są wykorzystywane przez nich sieci i systemy informatyczne. Uwzględniając najnowszy stan wiedzy, środki te muszą zapewniać poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do istniejącego ryzyka.

2. Państwa członkowskie zapewniają, aby operatorzy usług kluczowych podejmowali odpowiednie środki zapobiegające i minimalizujące wpływ incydentów dotyczących bezpieczeństwa sieci i systemów informatycznych wykorzystywanych w celu świadczenia takich usług kluczowych, z myślą o zapewnieniu ciągłości tych usług.

3. Państwa członkowskie zapewniają, aby operatorzy usług kluczowych niezwłocznie zgłaszali właściwemu organowi lub CSIRT incydenty mające istotny wpływ na ciągłość świadczonych przez nich usług kluczowych. Zgłoszenia muszą zawierać informacje umożliwiające właściwemu organowi lub CSIRT określenie transgranicznego wpływu incydentu. Zgłoszenie nie może narażać strony zgłaszającej na zwiększoną odpowiedzialność.

4. Aby określić istotność wpływu danego incydentu, uwzględnia się w szczególności następujące parametry:

a) liczbę użytkowników, których dotyczy zakłócenie usługi kluczowej;

b) czas trwania incydentu;

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

5. W oparciu o informacje przekazane w zgłoszeniu przez operatora usług kluczowych właściwy organ lub CSIRT informuje inne państwo członkowskie, którego dotyczy incydent, lub inne państwa członkowskie, których dotyczy incydent, czy ma on istotny wpływ na ciągłość usług kluczowych w tym państwie członkowskim. W działaniach tych właściwy organ lub CSIRT – zgodnie z prawem Unii lub prawodawstwem krajowym zgodnym z prawem Unii – chronią bezpieczeństwo i interesy handlowe operatora usług kluczowych, jak również poufność informacji przekazanych w jego zgłoszeniu.

Jeżeli pozwalają na to okoliczności, właściwy organ lub CSIRT przekazują zgłaszającemu operatorowi usług kluczowych odpowiednie informacje dotyczące działań następczych jego zgłoszenia, takie jak informacje, które mogłyby wesprzeć skuteczne postępowanie w przypadku incydentu.

Na wniosek właściwego organu lub CSIRT pojedynczy punkt kontaktowy przekazuje zgłoszenia, o których mowa w akapicie pierwszym, pojedynczym punktom kontaktowym w innych państwach członkowskich, których dotyczy incydent.

6. Po konsultacji ze zgłaszającym operatorem usług kluczowych właściwy organ lub CSIRT może poinformować społeczeństwo o poszczególnych incydentach, w przypadku gdy wiedza społeczeństwa jest niezbędna do tego, aby zapobiec wystąpieniu incydentu lub aby poradzić sobie z trwającym incydentem.

7. Właściwe organy, działając wspólnie w ramach grupy współpracy, mogą opracować i przyjąć wytyczne dotyczące okoliczności, w których operatorzy usług kluczowych są zobowiązani do zgłaszania incydentów, w tym parametry służące określeniu istotności wpływu incydentu, o której mowa w ust. 4.

Artykuł 15

Wdrażanie i egzekwowanie

1. Państwa członkowskie zapewniają, aby właściwe organy miały uprawnienia i środki niezbędne do oceny wypełniania przez operatorów usług kluczowych ich obowiązków na mocy art. 14 oraz jego skutków dla bezpieczeństwa sieci i systemów informatycznych.

2. Państwa członkowskie zapewniają, aby właściwe organy miały uprawnienia i środki, pozwalające wymagać od operatorów usług kluczowych przekazywania:

a) informacji niezbędnych do oceny bezpieczeństwa ich sieci i systemów informatycznych, w tym dokumentów dotyczących polityki w zakresie bezpieczeństwa;

b) dowodów skutecznej realizacji polityk w zakresie bezpieczeństwa, takich jak wyniki audytu bezpieczeństwa przeprowadzonego przez właściwy organ lub wykwalifikowanego audytora oraz, w tym ostatnim przypadku, udostępniania ich wyników – łącznie ze wspierającymi je dowodami – właściwemu organowi.

Zwracając się o przekazanie takich informacji lub dowodów, właściwy organ podaje cel wniosku i określa, jakie informacje są wymagane.

3. Po dokonaniu oceny informacji lub wyników audytów bezpieczeństwa, o których mowa w ust. 2, właściwy organ może wydać operatorom usług kluczowych wiążące polecenia wprowadzenia środków zaradczych w odniesieniu do stwierdzonych uchybień.

4. Obsługując incydenty, które doprowadziły do naruszeń danych osobowych, właściwy organ działa w ścisłej współpracy z organami ochrony danych.

ROZDZIAŁ V

BEZPIECZEŃSTWO SIECI I SYSTEMÓW INFORMATYCZNYCH DOSTAWCÓW USŁUG CYFROWYCH

Artykuł 16

Wymogi w zakresie bezpieczeństwa i zgłaszanie incydentów

1. Państwa członkowskie zapewniają, aby dostawcy usług cyfrowych określali i podejmowali odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykami, na jakie narażone są sieci i systemy informatyczne wykorzystywane przez nich w kontekście oferowania usług, o których mowa w załączniku III, w Unii. Uwzględniając najnowszy stan wiedzy, środki te muszą zapewniać poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do istniejącego ryzyka oraz uwzględniać następujące elementy:

a) bezpieczeństwo systemów i obiektów;

b) postępowanie w przypadku incydentu;

c) zarządzanie ciągłością działania;

d) monitorowanie, audyt i testowanie;

e) zgodność z normami międzynarodowymi.

2. Państwa członkowskie zapewniają, aby dostawcy usług cyfrowych podejmowali środki zapobiegające i minimalizujące wpływ incydentów dotyczących bezpieczeństwa ich sieci i systemów informatycznych na usługi, o których mowa w załączniku III, oferowane w Unii, z myślą o zapewnieniu ciągłości tych usług.

3. Państwa członkowskie zapewniają, aby dostawcy usług cyfrowych bez zbędnej zwłoki zgłaszali właściwemu organowi lub CSIRT wszelkie incydenty mające istotny wpływ na świadczenie usługi, o której mowa w załączniku III, oferowanej przez tych dostawców w Unii. Zgłoszenia muszą zawierać informacje umożliwiające właściwemu organowi lub CSIRT określenie istotności wpływu transgranicznego. Zgłoszenie nie może narażać strony zgłaszającej na zwiększoną odpowiedzialność.

4. W celu określenia, czy wpływ incydentu jest istotny, uwzględnia się w szczególności następujące parametry:

a) liczbę użytkowników, których dotyczy incydent, w szczególności użytkowników zależnych od usługi na potrzeby świadczenia ich własnych usług;

b) czas trwania incydentu;

c) zasięg geograficzny, którego dotyczy incydent;

d) zasięg zakłócenia funkcjonowania usługi;

e) zasięg wpływu na działalność gospodarczą i społeczną.

Obowiązek zgłoszenia incydentu ma zastosowanie wyłącznie wówczas, gdy dostawca usług cyfrowych ma dostęp do informacji niezbędnych do oceny wpływu incydentu względem parametrów, o których mowa w akapicie pierwszym.

5. W przypadku gdy do celów świadczenia usługi, która ma istotne znaczenie dla utrzymania krytycznej działalności społecznej i gospodarczej, operator usług kluczowych jest zależny od dostawcy usług cyfrowych będącego stroną trzecią, operatorowi temu zgłasza się wszelki istotny wpływ na ciągłość usług kluczowych związany z incydentem, który dotyczy dostawcy usług cyfrowych.

6. W stosownych przypadkach, w szczególności gdy incydent, o którym mowa w ust. 3, dotyczy dwóch lub większej liczby państw członkowskich, właściwy organ lub CSIRT informuje inne państwa członkowskie, których dotyczy incydent. W działaniach tych właściwe organy, CSIRT i pojedyncze punkty kontaktowe – zgodnie z prawem Unii lub prawodawstwem krajowym zgodnym z prawem Unii – chronią bezpieczeństwo i interesy handlowe dostawcy usług cyfrowych, jak również poufność przekazywanych informacji.

7. Po konsultacji z zainteresowanym dostawcą usług cyfrowych właściwy organ lub CSIRT oraz, w stosownych przypadkach, organy lub CSIRT innych zainteresowanych państw członkowskich mogą poinformować społeczeństwo o poszczególnych incydentach lub zobowiązać dostawcę usług cyfrowych, aby to zrobił, w przypadku gdy wiedza społeczeństwa jest niezbędna, żeby zapobiec wystąpieniu incydentu lub aby poradzić sobie z trwającym incydentem lub w przypadku gdy ujawnienie incydentu z innych względów leży w interesie publicznym.

8. Komisja przyjmuje akty wykonawcze w celu dalszego doprecyzowania elementów, o których mowa w ust. 1, oraz parametrów wymienionych w ust. 4 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 22 ust. 2, w terminie do dnia 9 sierpnia 2017 r.

9. Komisja może przyjąć akty wykonawcze określające formaty i procedury mające zastosowanie do wymogów dotyczących zgłaszania. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 22 ust. 2.

10. Bez uszczerbku dla art. 1 ust. 6 państwa członkowskie nie mogą nakładać na dostawców usług cyfrowych jakichkolwiek dalszych wymogów dotyczących bezpieczeństwa lub zgłaszania.

11. Rozdział V nie ma zastosowania do mikroprzedsiębiorstw i małych przedsiębiorstw zdefiniowanych w zaleceniu Komisji 2003/361/WE ([1]).

([1]) Zalecenie Komisji 2003/361/WE z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36).

Artykuł 17

Wdrażanie i egzekwowanie

1. Państwa członkowskie zapewniają, aby właściwe organy podjęły działania, w razie konieczności, w drodze środków nadzorczych *ex post*, gdy otrzymają dowód, że dostawca usług cyfrowych nie spełnia wymogów określonych w art. 16. Taki dowód może zostać przekazany przez właściwy organ innego państwa członkowskiego, w którym usługa jest świadczona.

2. Do celów ust. 1 właściwe organy muszą mieć uprawnienia i środki niezbędne do wymagania od dostawców usług cyfrowych:

a) przekazywania informacji niezbędnych do oceny bezpieczeństwa ich sieci i systemów informatycznych, w tym dokumentów dotyczących polityki w zakresie bezpieczeństwa;

b) eliminowania wszelkich przypadków niespełnienia wymogów określonych w art. 16.

3. Jeżeli dostawca usług cyfrowych posiada główną jednostkę organizacyjną lub przedstawiciela w jednym państwie członkowskim, ale jego sieć i systemy informatyczne są zlokalizowane w jednym lub większej liczbie innych państw członkowskich, właściwy organ państwa członkowskiego głównej jednostki organizacyjnej lub przedstawiciela oraz właściwe organy tych innych państw członkowskich współpracują ze sobą i udzielają sobie wzajemnie pomocy, odpowiednio do potrzeb. Taka pomoc i współpraca mogą obejmować wymianę informacji między zainteresowanymi właściwymi organami oraz wnioski o podjęcie środków nadzorczych, o których mowa w ust. 2.

Artykuł 18

Jurysdykcja i terytorialność

1. Na potrzeby niniejszej dyrektywy uznaje się, że dostawca usług cyfrowych podlega jurysdykcji państwa członkowskiego, w którym posiada główną jednostkę organizacyjną. Uznaje się, że dostawca usług cyfrowych posiada główną jednostkę organizacyjną w państwie członkowskim, gdy ma siedzibę zarządu w tym państwie członkowskim.

2. Dostawca usług cyfrowych, który nie posiada jednostki organizacyjnej w Unii, ale oferuje usługi, o których mowa w załączniku III, w Unii, wyznacza przedstawiciela w Unii. Przedstawiciel musi posiadać jednostkę organizacyjną w jednym z tych państw członkowskich, w których oferowane są usługi. Uznaje się, że dostawca usług cyfrowych podlega jurysdykcji państwa członkowskiego, w którym przedstawiciel posiada jednostkę organizacyjną.

3. Wyznaczenie przedstawiciela przez dostawcę usług cyfrowych pozostaje bez uszczerbku dla działań prawnych, które mogłyby zostać podjęte przeciwko samemu dostawcy usług cyfrowych.

ROZDZIAŁ VI

NORMALIZACJA I DOBROWOLNE ZGŁASZANIE INCYDENTÓW

Artykuł 19

Normalizacja

1. Aby wspierać spójne wdrażanie art. 14 ust. 1 i 2 oraz art. 16 ust. 1 i 2, państwa członkowskie, nie narzucając ani nie faworyzując wykorzystywania określonego rodzaju technologii, zachęcają do stosowania europejskich lub uznanych międzynarodowo norm i specyfikacji mających znaczenie dla bezpieczeństwa sieci i systemów informatycznych.

2. ENISA, we współpracy z państwami członkowskimi, opracowuje porady i wytyczne dotyczące kwestii technicznych, które powinny zostać wzięte pod uwagę w odniesieniu do ust. 1, a także dotyczące już istniejących norm, w tym krajowych norm państw członkowskich, które pozwoliłyby na uwzględnienie tych obszarów.

Artykuł 20

Dobrowolne zgłaszanie incydentów

1. Bez uszczerbku dla art. 3 podmioty, które nie zostały zidentyfikowane jako operatorzy usług kluczowych i które nie są dostawcami usług cyfrowych, mogą na zasadzie dobrowolności zgłaszać incydenty mające istotny wpływ na ciągłość usług, które świadczą.

2. Przy rozpatrywaniu zgłoszeń państwa członkowskie postępują zgodnie z procedurą określoną w art. 14. Państwa członkowskie mogą rozpatrywać zgłoszenia obowiązkowe priorytetowo względem zgłoszeń dobrowolnych. Zgłoszenia dobrowolne są rozpatrywane wyłącznie wtedy, gdy takie rozpatrywanie nie stanowi nieproporcjonalnego czy nadmiernego obciążenia dla danych państw członkowskich.

Zgłoszenie dobrowolne nie może skutkować nałożeniem na podmiot zgłaszający jakichkolwiek obowiązków, którym by nie podlegał, gdyby nie dokonał tego zgłoszenia.

ROZDZIAŁ VII

PRZEPISY KOŃCOWE

Artykuł 21

Sankcje

Państwa członkowskie ustanawiają przepisy dotyczące sankcji mających zastosowanie w przypadku naruszeń krajowych przepisów przyjętych na podstawie niniejszej dyrektywy i podejmują wszystkie niezbędne środki w celu zapewnienia ich wykonania. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie powiadamiają Komisję o tych przepisach i środkach do dnia 9 maja 2018 r., a także powiadamiają ją niezwłocznie o wszelkich późniejszych zmianach, które ich dotyczą.

Artykuł 22

Procedura komitetowa

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

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

Artykuł 23

Przegląd

1. W terminie do dnia 9 maja 2019 r. Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie, w którym oceni spójność podejścia przyjętego przez państwa członkowskie do identyfikacji operatorów usług kluczowych.

2. Komisja dokonuje okresowego przeglądu funkcjonowania niniejszej dyrektywy i składa Parlamentowi Europejskiemu i Radzie sprawozdania na ten temat. W tym celu oraz z myślą o dalszym rozwijaniu współpracy strategicznej i operacyjnej Komisja bierze pod uwagę sprawozdania grupy współpracy i sieci CSIRT na temat doświadczeń zdobytych na poziomie strategicznym i operacyjnym. W swoim przeglądzie Komisja oceni również wykazy zawarte w załącznikach II i III oraz spójność w identyfikacji operatorów usług kluczowych oraz usług w sektorach, o których mowa w załączniku II. Pierwsze sprawozdanie zostanie przedłożone w terminie do dnia 9 maja 2021 r.

Artykuł 24

Środki przejściowe

1. Bez uszczerbku dla art. 25 oraz w celu zapewnienia państwom członkowskim dodatkowych możliwości odpowiedniej współpracy podczas okresu transpozycji grupa współpracy i sieć CSIRT rozpoczynają wykonywanie swoich zadań określonych, odpowiednio, w art. 11 ust. 3 i art. 12 ust. 3 w terminie do dnia 9 lutego 2017 r.

2. W okresie od dnia 9 lutego 2017 r. do dnia 9 listopada 2018 r. oraz w celu wspierania państw członkowskich w przyjmowaniu spójnego podejścia w procesie identyfikacji operatorów usług kluczowych grupa współpracy omawia ten proces, treść i rodzaj środków krajowych umożliwiających identyfikację operatorów usług kluczowych w danym sektorze zgodnie z kryteriami określonymi w art. 5 i 6. Grupa współpracy omawia również, na wniosek państwa członkowskiego, konkretne projekty środków krajowych tego państwa członkowskiego, umożliwiając identyfikację operatorów usług kluczowych w danym sektorze zgodnie z kryteriami określonymi w art. 5 i 6.

3. W terminie do dnia 9 lutego 2017 r. oraz do celów niniejszego artykułu państwa członkowskie zapewnią właściwą reprezentację w grupie współpracy i w sieci CSIRT.

Artykuł 25

Transpozycja

1. Państwa członkowskie przyjmują i publikują w terminie do dnia 9 maja 2018 r. przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy. Niezwłocznie powiadamiają o tym Komisję.

Państwa członkowskie stosują te środki od dnia 10 maja 2018 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.

2. Państwa członkowskie przekazują Komisji teksty podstawowych przepisów prawa krajowego przyjętych w dziedzinie objętej niniejszą dyrektywą.

Artykuł 26

Wejście w życie

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

Artykuł 27

Adresaci

Niniejsza dyrektywa skierowana jest do państw członkowskich.

Sporządzono w Strasburgu dnia 6 lipca 2016 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
M. SCHULZ	I. KORČOK
Przewodniczący	*Przewodniczący*

ZAŁĄCZNIK I

WYMOGI DOTYCZĄCE ZESPOŁÓW REAGOWANIA NA INCYDENTY BEZPIECZEŃSTWA KOMPUTEROWEGO (CSIRT) I ICH ZADANIA

Wymogi dotyczące CSIRT i ich zadania muszą być odpowiednio i jasno określone i umocowane w politykach lub regulacjach krajowych. Muszą one obejmować:

1) Wymogi dotyczące CSIRT:

   a) CSIRT muszą zapewniać wysoką dostępność swoich usług łączności poprzez unikanie pojedynczych punktów awarii oraz dysponować różnymi kanałami, za pomocą których zawsze można się z nimi skontaktować i za pomocą których one same mogą się kontaktować z innymi. Ponadto kanały komunikacyjne muszą być wyraźnie określone i dobrze znane wśród użytkowników CSIRT i wśród współpracujących partnerów;

   b) Pomieszczenia CSIRT oraz wspierające systemy informatyczne muszą być zlokalizowane w bezpiecznych miejscach;

   c) Ciągłość działania:

      (i) CSIRT muszą być wyposażone w odpowiedni system zarządzania i sterowania wnioskami w celu ułatwienia ich późniejszego przekazywania;

      (ii) CSIRT muszą dysponować odpowiednią liczbą personelu, aby zapewnić nieprzerwaną dostępność;

      (iii) CSIRT muszą być zależne od infrastruktury o zapewnionej ciągłości działania. W tym celu muszą być dostępne systemy redundantne i zapasowa przestrzeń robocza;

   d) CSIRT muszą mieć możliwość udziału, w stosownych przypadkach, w międzynarodowych sieciach współpracy.

2) Zadania CSIRT:

   a) Zadania CSIRT muszą obejmować co najmniej:

      (i) monitorowanie incydentów na poziomie krajowym;

      (ii) przekazywanie zainteresowanym stronom wczesnych ostrzeżeń, ogłaszanie alarmów, wydawanie ogłoszeń i przekazywanie informacji skierowanych do zainteresowanych stron, dotyczących ryzyk i incydentów;

      (iii) reagowanie na incydenty;

      (iv) zapewnianie dynamicznej analizy ryzyka i incydentów oraz orientacji sytuacyjnej;

      (v) udział w sieci CSIRT;

   b) CSIRT musi nawiązać współpracę z sektorem prywatnym;

   c) W celu ułatwienia współpracy CSIRT musi wspierać przyjmowanie i wykorzystywanie wspólnych lub znormalizowanych praktyk w odniesieniu do:

      (i) procedur postępowania w przypadku incydentu i wystąpienia ryzyka;

      (ii) systemów klasyfikacji incydentów, ryzyka i informacji.

ZAŁĄCZNIK II

RODZAJE PODMIOTÓW DO CELÓW ART. 4 PKT 4

Sektor	Podsektor	Rodzaj podmiotu
1. Energetyka	a) Energia elektryczna	— przedsiębiorstwa energetyczne zgodnie z definicją w art. 2 pkt 35 dyrektywy Parlamentu Europejskiego i Rady 2009/72/WE ([1]), które wykonują funkcję „dostawy" zgodnie z definicją w art. 2 pkt 19 tej dyrektywy
		— operatorzy systemu dystrybucyjnego zgodnie z definicją w art. 2 pkt 6 dyrektywy 2009/72/WE
		— operatorzy systemu przesyłowego zgodnie z definicją w art. 2 pkt 4 dyrektywy 2009/72/WE
	b) Ropa naftowa	— operatorzy ropociągów
		— operatorzy instalacji służących do produkcji, rafinacji, przetwarzania, magazynowania i przesyłu ropy naftowej
	c) Gaz	— przedsiębiorstwa dostarczające gaz zgodnie z definicją w art. 2 pkt 8 dyrektywy Parlamentu Europejskiego i Rady 2009/73/WE ([2])
		— operatorzy systemu dystrybucyjnego zgodnie z definicją w art. 2 pkt 6 dyrektywy 2009/73/WE
		— operatorzy systemu przesyłowego zgodnie z definicją w art. 2 pkt 4 dyrektywy 2009/73/WE
		— operatorzy systemu magazynowania zgodnie z definicją w art. 2 pkt 10 dyrektywy 2009/73/WE
		— operatorzy systemu LNG zgodnie z definicją w art. 2 pkt 12 dyrektywy 2009/73/WE
		— przedsiębiorstwa gazowe zgodnie z definicją w art. 2 pkt 1 dyrektywy 2009/73/WE
		— operatorzy instalacji służących do rafinacji i przetwarzania gazu ziemnego
2. Transport	a) Transport lotniczy	— przewoźnicy lotniczy zgodnie z definicją w art. 3 pkt 4 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 300/2008 ([3])
		— zarządzający portem lotniczym zgodnie z definicją w art. 2 pkt 2 dyrektywy Parlamentu Europejskiego i Rady 2009/12/WE ([4]), porty lotnicze zgodnie z definicją w art. 2 pkt 1 tej dyrektywy, w tym porty bazowe wymienione w sekcji 2 załącznika II do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1315/2013 ([5]); oraz jednostki obsługujące urządzenia pomocnicze znajdujące się w portach lotniczych

Sektor	Podsektor	Rodzaj podmiotu
		— operatorzy zarządzający ruchem lotniczym zapewniający służbę kontroli ruchu lotniczego (ATC) zgodnie z definicją w art. 2 pkt 1 rozporządzenia (WE) nr 549/2004 Parlamentu Europejskiego i Rady ([6])
	b) Transport kolejowy	— zarządcy infrastruktury zgodnie z definicją w art. 3 pkt 2 dyrektywy Parlamentu Europejskiego i Rady 2012/34/UE ([7]);
		— przedsiębiorstwa kolejowe zgodnie z definicją w art. 3 pkt 1 dyrektywy 2012/34/UE, w tym operatorzy obiektów infrastruktury usługowej zgodnie z definicją w art. 3 pkt 12 dyrektywy 2012/34/UE
	c) Transport wodny	— armatorzy śródlądowego, morskiego i przybrzeżnego wodnego transportu pasażerów i towarów zgodnie z definicją dla transportu morskiego w załączniku I do rozporządzenia (WE) nr 725/2004 Parlamentu Europejskiego i Rady ([8]), z wyłączeniem poszczególnych statków, na których prowadzą działalność ci armatorzy
		— organy zarządzające portami zgodnie z definicją w art. 3 pkt 1 dyrektywy 2005/65/WE Parlamentu Europejskiego i Rady ([9]), w tym ich obiekty portowe zgodnie z definicją w art. 2 pkt 11 rozporządzenia (WE) nr 725/2004; oraz jednostki wykonujące prace i operujące sprzętem znajdującym się w tych portach
		— operatorzy systemów ruchu statków zgodnie z definicją w art. 3 lit. o) dyrektywy 2002/59/WE Parlamentu Europejskiego i Rady ([10])
	d) Transport drogowy	— organy administracji drogowej zgodnie z definicją w art. 2 pkt 12 rozporządzenia delegowanego Komisji (UE) 2015/962 ([11]) odpowiedzialne za zarządzanie ruchem drogowym
		— operatorzy inteligentnych systemów transportowych zgodnie z definicją w art. 4 pkt 1 dyrektywy Parlamentu Europejskiego i Rady 2010/40/WE ([12])
3. Bankowość		instytucje kredytowe zgodnie z definicją w art. 4 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 575/2013 ([13])
4. Infrastruktura rynków finansowych		— operatorzy systemu obrotu zgodnie z definicją w art. 4 pkt 24 dyrektywy Parlamentu Europejskiego i Rady 2014/65/UE ([14])
		— kontrahenci centralni zgodnie z definicją w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 648/2012 ([15])
5. Służba zdrowia	Ośrodki opieki zdrowotnej (w tym szpitale i prywatne kliniki)	świadczeniodawcy zgodnie z definicją w art. 3 lit. g) dyrektywy Parlamentu Europejskiego i Rady 2011/24/UE ([16])

Sektor	Podsektor	Rodzaj podmiotu
6. Zaopatrzenie w wodę pitną i jej dystrybucja		dostawcy i dystrybutorzy „wody przeznaczonej do spożycia przez ludzi" zgodnie z definicją w art. 2 pkt 1 lit. a) dyrektywy Rady 98/83/WE ([17]), ale z wyłączeniem dystrybutorów, dla których dystrybucja wody przeznaczonej do spożycia przez ludzi jest jedynie częścią ich ogólnej działalności polegającej na dystrybucji innych produktów i towarów, które nie są uznawane za usługi kluczowe
7. Infrastruktura cyfrowa		— IXP
		— dostawcy usług DNS
		— rejestry nazw TLD

([1]) Dyrektywa Parlamentu Europejskiego i Rady 2009/72/WE z dnia 13 lipca 2009 r. dotycząca wspólnych zasad rynku wewnętrznego energii elektrycznej i uchylająca dyrektywę 2003/54/WE (Dz.U. L 211 z 14.8.2009, s. 55).
([2]) Dyrektywa Parlamentu Europejskiego i Rady 2009/73/WE z dnia 13 lipca 2009 r. dotycząca wspólnych zasad rynku wewnętrznego gazu ziemnego i uchylająca dyrektywę 2003/55/WE (Dz.U. L 211 z 14.8.2009, s. 94).
([3]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002 (Dz.U. L 97 z 9.4.2008, s. 72).
([4]) Dyrektywa Parlamentu Europejskiego i Rady 2009/12/WE z dnia 11 marca 2009 r. w sprawie opłat lotniskowych (Dz.U. L 70 z 14.3.2009, s. 11).
([5]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1315/2013 z dnia 11 grudnia 2013 r. w sprawie unijnych wytycznych dotyczących rozwoju transeuropejskiej sieci transportowej i uchylające decyzję nr 661/2010/UE (Dz.U. L 348 z 20.12.2013, s. 1).
([6]) Rozporządzenie (WE) nr 549/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiające ramy tworzenia Jednolitej Europejskiej Przestrzeni Powietrznej (Rozporządzenie ramowe) (Dz.U. L 96 z 31.3.2004, s. 1).
([7]) Dyrektywa Parlamentu Europejskiego i Rady 2012/34/UE z dnia 21 listopada 2012 r. w sprawie utworzenia jednolitego europejskiego obszaru kolejowego (Dz.U. L 343 z 14.12.2012, s. 32).
([8]) Rozporządzenie (WE) nr 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych (Dz.U. L 129 z 29.4.2004, s. 6).
([9]) Dyrektywa 2005/65/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie wzmocnienia ochrony portów (Dz.U. L 310 z 25.11.2005, s. 28).
([10]) Dyrektywa 2002/59/WE Parlamentu Europejskiego i Rady z dnia 27 czerwca 2002 r. ustanawiająca wspólnotowy system monitorowania i informacji o ruchu statków i uchylająca dyrektywę Rady 93/75/EWG (Dz.U. L 208 z 5.8.2002, s. 10).
([11]) Rozporządzenie delegowane Komisji (UE) 2015/962 z dnia 18 grudnia 2014 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2010/40/UE w odniesieniu do świadczenia ogólnounijnych usług informacyjnych w czasie rzeczywistym dotyczących ruchu (Dz.U. L 157 z 23.6.2015, s. 21).
([12]) Dyrektywa Parlamentu Europejskiego i Rady 2010/40/UE z dnia 7 lipca 2010 r. w sprawie ram wdrażania inteligentnych systemów transportowych w obszarze transportu drogowego oraz interfejsów z innymi rodzajami transportu (Dz.U. L 207 z 6.8.2010, s. 1).
([13]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012 (Dz.U. L 176 z 27.6.2013, s. 1).
([14]) Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE (Dz.U. L 173 z 12.6.2014, s. 349).
([15]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 z dnia 4 lipca 2012 r. w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji (Dz.U. L 201 z 27.7.2012, s. 1).
([16]) Dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE z dnia 9 marca 2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej (Dz.U. L 88 z 4.4.2011, s. 45).
([17]) Dyrektywa Rady 98/83/WE z dnia 3 listopada 1998 r. w sprawie jakości wody przeznaczonej do spożycia przez ludzi (Dz.U. L 330 z 5.12.1998, s. 32).

ZAŁĄCZNIK III

RODZAJE USŁUG CYFROWYCH DO CELÓW ART. 4 PKT 5

1. Internetowa platforma handlowa.
2. Wyszukiwarka internetowa.
3. Usługa przetwarzania w chmurze.