KOMISJA
EUROPEJSKA

Bruksela, dnia 4.10.2017 r.
COM(2017) 476 final

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

# KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

## Pełne wykorzystanie potencjału bezpieczeństwa sieci i informacji - zapewnienie skutecznego wdrożenia dyrektywy (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii

PL

## Wprowadzenie

Przyjęta w dniu 6 lipca 2016 r. dyrektywa (UE) 2016/1148 w sprawie bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[1] (zwana dalej „dyrektywą w sprawie bezpieczeństwa sieci i informacji" lub „dyrektywą") jest pierwszym horyzontalnym unijnym aktem prawnym stanowiącym odpowiedź na wyzwania w obszarze cyberbezpieczeństwa, który wprowadza rzeczywiste zmiany w kwestii odporności na zagrożenia dla cyberbezpieczeństwa i współpracy w dziedzinie cyberbezpieczeństwa w Europie.

Dyrektywa ma trzy główne cele:

- poprawa zdolności do podejmowania działań w obszarze cyberbezpieczeństwa na szczeblu krajowym;
- rozwijanie współpracy na szczeblu unijnym; oraz
- propagowanie kultury zarządzania ryzykiem i zgłaszania incydentów wśród najważniejszych podmiotów gospodarczych, w szczególności operatorów usług kluczowych dla utrzymania działalności gospodarczej i społecznej oraz dostawców usług cyfrowych.

Dyrektywa w sprawie bezpieczeństwa sieci i informacji leży u podstaw działań podejmowanych przez UE w odpowiedzi na coraz poważniejsze zagrożenia i wyzwania cybernetyczne towarzyszące cyfryzacji życia gospodarczego i społecznego, dlatego też jej wdrożenie stanowi zasadniczy element pakietu „Bezpieczeństwo cybernetyczne" przedstawionego w dniu 13 września 2017 r. Skuteczność działań podejmowanych przez UE w reakcji na te zagrożenia i wyzwania będzie ograniczona, dopóki dyrektywa w sprawie bezpieczeństwa sieci i informacji nie zostanie w pełni transponowana we wszystkich państwach członkowskich UE. Kwestię tę uznano również za kluczową w komunikacie Komisji z 2016 r. w sprawie wzmacniania europejskiego systemu odporności cybernetycznej[2].

Nowatorski charakter dyrektywy w sprawie bezpieczeństwa sieci i informacji oraz konieczność pilnego zaradzenia szybko ewoluującym zagrożeniom cybernetycznym uzasadniają zwrócenie szczególnej uwagi na stojące przed wszystkimi zainteresowanymi podmiotami wyzwania związane z zapewnieniem terminowej i pomyślnej transpozycji dyrektywy. Z uwagi na fakt, że termin transpozycji upływa w dniu 9 maja 2018 r., a termin na zidentyfikowanie operatorów usług kluczowych – w dniu 9 listopada 2018 r., Komisja udziela państwom członkowskim wsparcia w procesie transpozycji oraz wspiera podejmowane przez nie starania w tym zakresie w ramach grupy współpracy.

Niniejszy komunikat oraz towarzyszący mu załącznik zostały opracowane na podstawie przeprowadzonych przez Komisję prac przygotowawczych i analizy, związanych

[1] 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. Dyrektywa ta weszła w życie z dniem 8 sierpnia 2016 r.
[2] COM(2016) 410 final.

z dotychczasowymi postępami we wdrażaniu dyrektywy w sprawie bezpieczeństwa sieci i informacji, na podstawie informacji przekazanych przez Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz na podstawie rozmów z państwami członkowskimi, jakie odbyły się na etapie transpozycji dyrektywy, w szczególności na forum grupy współpracy[3]. Niniejszy komunikat stanowi uzupełnienie dotychczasowych istotnych starań w tym obszarze, w szczególności obejmujących:

- intensywne prace prowadzone na forum grupy współpracy, która uzgodniła plan prac ukierunkowany przede wszystkim na transpozycję dyrektywy w sprawie bezpieczeństwa sieci i informacji, w szczególności na kwestię identyfikacji operatorów usług kluczowych oraz spoczywających na nich obowiązków dotyczących wymogów w zakresie bezpieczeństwa i zgłaszania incydentów. Chociaż w dyrektywie przewidziano swobodę uznania, jeżeli chodzi o transpozycję przepisów dotyczących operatorów usług kluczowych, państwa członkowskie uznały znaczenie zharmonizowanego podejścia do tej kwestii[4];
- ustanowienie i zapewnienie sprawnego funkcjonowania sieci zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) zgodnie z art. 12 ust. 1 dyrektywy. Od chwili ustanowienia sieć ta zaczęła tworzyć podwaliny pod ustrukturyzowaną współpracę operacyjną na szczeblu europejskim.

Pełne zaangażowanie wszystkich państw członkowskich zarówno na szczeblu polityki, jak i na szczeblu operacyjnym, które to szczeble reprezentują obie wspomniane powyżej struktury, ma zasadnicze znaczenie dla osiągnięcia celu polegającego na zapewnieniu wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

Niniejszy komunikat i towarzyszący mu załącznik zintensyfikują starania podejmowane w tym obszarze, ponieważ zebrano w nich i porównano najlepsze praktyki z państw członkowskich istotne w kontekście wdrożenia dyrektywy, przekazano dodatkowe wytyczne dotyczące sposobu, w jaki należy wdrażać dyrektywę, oraz przedstawiono bardziej szczegółowe wyjaśnienia dotyczące poszczególnych przepisów. Nadrzędnym celem jest wsparcie państw członkowskich w osiągnięciu skutecznego i zharmonizowanego wdrożenia dyrektywy w sprawie bezpieczeństwa sieci i informacji w całej UE.

Niniejszy komunikat zostanie dodatkowo uzupełniony przygotowywanym rozporządzeniem wykonawczym Komisji w sprawie doprecyzowania elementów i parametrów związanych z wymogami w zakresie bezpieczeństwa i zgłaszania incydentów dla dostawców usług cyfrowych na podstawie art. 16 ust. 8 dyrektywy w sprawie bezpieczeństwa sieci i informacji.

[3] Mechanizm strategicznej współpracy między państwami członkowskimi na mocy art. 11 dyrektywy w sprawie bezpieczeństwa sieci i informacji.

[4] Grupa współpracy pracuje obecnie nad wytycznymi referencyjnymi, które dotyczą m.in.: kryteriów, na podstawie których danego operatora można uznać za operatora usług kluczowych zgodnie z art. 5 ust. 2 dyrektywy; okoliczności, w których operatorzy usług kluczowych są zobowiązani do zgłaszania incydentów na podstawie art. 14 ust. 7 dyrektywy; oraz wymogów w zakresie bezpieczeństwa spoczywających na operatorach usług kluczowych zgodnie z art. 14 ust. 1 i 2.

Wspomniane rozporządzenie wykonawcze ułatwi wdrożenie dyrektywy w odniesieniu do obowiązków spoczywających na dostawcach usług cyfrowych[5].

W niniejszym komunikacie przedstawiono najistotniejsze wnioski z analizy zagadnień, które są postrzegane jako ważne punkty odniesienia i potencjalne źródła inspiracji w kontekście transpozycji dyrektywy do prawa krajowego. W tym kontekście skoncentrowano się przede wszystkim na przepisach dotyczących zdolności państw członkowskich i spoczywających na nich zobowiązań względem podmiotów objętych zakresem stosowania dyrektywy. W załączniku przeprowadzono bardziej szczegółową analizę tych obszarów, które Komisja uznała za najbardziej wartościowe źródło praktycznych wytycznych dotyczących procesu transpozycji, poprzez wyjaśnianie i interpretowanie określonych przepisów dyrektywy oraz poprzez przedstawianie zgromadzonych dotychczas najlepszych praktyk i doświadczeń związanych z dyrektywą.

## Zapewnienie skutecznego wdrożenia dyrektywy w sprawie bezpieczeństwa sieci i informacji

Celem dyrektywy w sprawie bezpieczeństwa sieci i informacji jest zapewnienie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w całej UE. Oznacza to poprawę bezpieczeństwa internetu i sieci prywatnych oraz systemów informatycznych o kluczowym znaczeniu dla funkcjonowania naszego społeczeństwa i gospodarki. Pierwszym istotnym elementem w tym zakresie jest gotowość państw członkowskich, którą powinno się zagwarantować przez przyjmowanie opisanych w dyrektywie krajowych strategii bezpieczeństwa cybernetycznego oraz w drodze odpowiednich działań podejmowanych przez CSIRT i właściwe organy krajowe.

*Kompleksowość strategii krajowych*

Ważne jest, aby państwa członkowskie wykorzystały transpozycję dyrektywy w sprawie bezpieczeństwa sieci i informacji jako okazję do przeprowadzenia przeglądu swoich krajowych strategii bezpieczeństwa cybernetycznego pod kątem luk, najlepszych praktyk i nowych wyzwań wskazanych w załączniku.

Chociaż w dyrektywie ze zrozumiałych względów skoncentrowano się na przedsiębiorstwach i usługach o szczególnie kluczowym znaczeniu, należy pamiętać o konieczności zadbania o cyberbezpieczeństwo gospodarki i społeczeństwa ogółem w całościowy i spójny sposób, zważywszy na coraz większą zależność od technologii informacyjno-komunikacyjnych. Dlatego też przyjęcie kompleksowych strategii krajowych wykraczających poza minimalne wymogi ustanowione w dyrektywie w sprawie bezpieczeństwa sieci i informacji (tj. obejmujących nie tylko sektory i usługi wymienione, odpowiednio, w załącznikach II i III do dyrektywy) poprawiłoby ogólny poziom bezpieczeństwa sieci i systemów informatycznych.

[5] Projekt rozporządzenia wykonawczego udostępniono do celów konsultacji publicznych na stronie: https://ec.europa.eu/info/law/better-regulation/have-your-say_en

Ponieważ cyberbezpieczeństwo nadal stanowi stosunkowo nowy i dynamicznie rozwijający się obszar polityki publicznej, w większości przypadków wymagane są nowe inwestycje, nawet jeśli ogólny stan finansów publicznych wskazuje raczej na konieczność dokonywania cięć i szukania oszczędności. Podejmowanie ambitnych decyzji w celu zapewnienia odpowiednich zasobów finansowych i ludzkich niezbędnych do skutecznego wdrożenia strategii krajowych, w tym zapewnienie dostatecznych zasobów właściwym organom krajowym i CSIRT, ma zatem kluczowe znaczenie dla osiągnięcia celów dyrektywy.

*Skuteczność wdrażania i egzekwowania*

Określony w art. 8 dyrektywy wymóg wyznaczenia odpowiednich właściwych organów krajowych i pojedynczych punktów kontaktowych ma zasadnicze znaczenie dla zagwarantowania skutecznego wdrożenia dyrektywy w sprawie bezpieczeństwa sieci i informacji oraz prowadzenia współpracy transgranicznej. W tym kontekście w państwach członkowskich pojawiły się podejścia zarówno bardziej scentralizowane, jak i bardziej zdecentralizowane. W przypadkach, w których państwa członkowskie przyjmują bardziej zdecentralizowane podejście do kwestii wyznaczania właściwych organów krajowych, okazało się, że podstawowe znaczenie ma zapewnienie przyjęcia solidnych rozwiązań dotyczących współpracy pomiędzy licznymi organami a pojedynczym punktem kontaktowym (*zob. tabela 1 w pkt 3.2 załącznika*). Rozwiązania takie zwiększyłyby skuteczność wdrażania dyrektywy oraz ułatwiłyby egzekwowanie jej przepisów.

Wykorzystanie wcześniejszych doświadczeń związanych z ochroną krytycznej infrastruktury teleinformatycznej może pomóc w opracowaniu optymalnego modelu zarządzania dla państw członkowskich, który zapewni zarówno skuteczne wdrożenie dyrektywy w sprawie bezpieczeństwa sieci i informacji w poszczególnych sektorach, jak i stosowanie spójnego podejścia horyzontalnego (*zob. pkt 3.1 załącznika*).

*Zwiększone zdolności krajowych CSIRT*

W przypadku nieutworzenia skutecznych i zaopatrzonych w odpowiednie zasoby krajowych CSIRT w całej UE, które przewidziano w art. 9 dyrektywy w sprawie bezpieczeństwa sieci i informacji, UE pozostanie w nadmiernym stopniu narażona na transgraniczne zagrożenia cybernetyczne. Dlatego też państwa członkowskie mogłyby rozważyć rozszerzenie zakresu działalności CSIRT poza sektory i usługi objęte zakresem stosowania dyrektywy (*zob. pkt 3.3 załącznika*). Dzięki temu krajowe CSIRT mogłyby udzielać wsparcia operacyjnego w związku z incydentami cybernetycznymi, do których dochodzi w przedsiębiorstwach i organizacjach nieobjętych zakresem stosowania dyrektywy, ale mimo to istotnych dla społeczeństwa i gospodarki. Ponadto państwa członkowskie mogłyby w pełni wykorzystać możliwości pozyskania dodatkowego finansowania, jakie oferuje program infrastruktury usług cyfrowych (DSI) w zakresie bezpieczeństwa cybernetycznego w ramach instrumentu

„Łącząc Europę”, którego celem jest zwiększanie zdolności krajowych CSIRT i zacieśnianie współpracy między nimi (*zob. pkt 3.5 załącznika*).

*Spójność procesu identyfikowania operatorów usług kluczowych*

Zgodnie z art. 5 dyrektywy w sprawie bezpieczeństwa sieci i informacji państwa członkowskie są zobowiązane do zidentyfikowania podmiotów, które będą uznawane za operatorów usług kluczowych, do dnia 9 listopada 2018 r. Przy wywiązywaniu się z tego obowiązku państwa członkowskie mogłyby rozważyć spójne stosowanie definicji i wytycznych zawartych w niniejszym komunikacie w celu zagwarantowania, aby podobnego rodzaju podmioty odgrywające podobną rolę na rynku wewnętrznym były spójnie identyfikowane jako operatorzy usług kluczowych w innych państwach członkowskich. Państwa członkowskie mogłyby również rozważyć rozszerzenie zakresu stosowania dyrektywy w sprawie bezpieczeństwa sieci i informacji na administracje publiczne, biorąc pod uwagę ich znaczenie dla społeczeństwa i gospodarki ogółem (*zob. pkt 2.1 i 4.1.3 załącznika*).

Bardzo przydatne byłoby maksymalne ujednolicenie krajowych podejść do identyfikowania operatorów usług kluczowych, w szczególności zgodnie z wytycznymi opracowanymi przez grupę współpracy (*zob. pkt 4.1.2 załącznika*), ponieważ doprowadziłoby to do bardziej zharmonizowanego stosowania przepisów dyrektywy, a tym samym do ograniczenia ryzyka fragmentacji rynku. W przypadkach, w których operatorzy usług kluczowych świadczą usługi kluczowe w co najmniej dwóch państwach członkowskich, niezbędne jest dążenie do osiągnięcia porozumienia między państwami członkowskimi w kontekście procesu konsultacji prowadzonego na podstawie art. 5 ust. 4 co do spójnego identyfikowania podmiotów (*zob. pkt 4.1.7 załącznika*), ponieważ pozwoliłoby to uniknąć rozbieżności w sposobie traktowania tego samego podmiotu w ramach jurysdykcji różnych państw członkowskich.

*Przekazywanie Komisji informacji na temat identyfikowania operatorów usług kluczowych*

W art. 5 ust. 7 wzywa się państwa członkowskie do przekazywania Komisji informacji na temat krajowych środków umożliwiających identyfikowanie operatorów usług kluczowych, wykazów usług kluczowych oraz danych dotyczących liczby zidentyfikowanych operatorów usług kluczowych i znaczenia tych operatorów dla sektora. Ponadto wzywa się państwa członkowskie do przekazywania informacji o progach, jeżeli istnieją, wykorzystywanych w ramach procesu identyfikowania w celu określenia odpowiedniego poziomu dostaw lub znaczenia konkretnego operatora dla utrzymania wystarczającego poziomu dostaw. Państwa członkowskie mogłyby również rozważyć udostępnianie Komisji wykazów zidentyfikowanych operatorów usług kluczowych, w razie konieczności na zasadzie poufności, ponieważ pomogłoby to w zwiększeniu trafności i jakości oceny przeprowadzanej przez Komisję (*zob. pkt 4.1.5 i 4.1.6 załącznika*).

*Ujednolicone podejścia do spoczywających na operatorach usług kluczowych wymogów w zakresie bezpieczeństwa i zgłaszania incydentów*

Jeżeli chodzi o obowiązki dotyczące spoczywających na operatorach usług kluczowych wymogów w zakresie bezpieczeństwa i zgłaszania incydentów (art. 14 ust. 1, 2 i 3), stosowanie ujednoliconego podejścia do wymogów w zakresie bezpieczeństwa i zgłaszania incydentów w celu ułatwienia operatorom usług kluczowych zapewniania zgodności z przepisami poza granicami państw członkowskich UE usprawniłoby w maksymalnym stopniu funkcjonowanie jednolitego rynku. Należy tutaj wspomnieć o pracy nad wytycznymi na forum grupy współpracy (*zob. pkt 4.2 i 4.3 załącznika*).

W przypadku wystąpienia incydentu cybernetycznego na dużą skalę, który wywiera wpływ na szereg państw członkowskich, istnieje bardzo duże prawdopodobieństwo, że obowiązkowe zgłoszenie incydentu zostanie dokonane przez operatora usług kluczowych lub dostawcę usług cyfrowych zgodnie z art. 14 ust. 3 i art. 16 ust. 3 lub przez inny podmiot nieobjęty zakresem stosowania dyrektywy na zasadzie dobrowolności, na podstawie art. 20 ust. 1. Zgodnie z zaleceniem Komisji w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę państwa członkowskie mogłyby rozważyć ujednolicenie swoich podejść krajowych w taki sposób, aby zagwarantować jak najszybsze przekazywanie odpowiednich informacji na podstawie tych zgłoszeń właściwym organom lub CSIRT innych zainteresowanych państw członkowskich. Przekazywanie precyzyjnych informacji, na podstawie których można podejmować stosowne działania, miałoby zasadnicze znaczenie dla ograniczenia liczby infekcji lub wyeliminowania słabych punktów, zanim zostaną one wykorzystane.

Działając w duchu partnerstwa i dążąc do wykorzystania w pełni potencjału dyrektywy w sprawie bezpieczeństwa sieci i informacji, Komisja zamierza rozszerzyć wsparcie udzielane w ramach instrumentu „Łącząc Europę” na wszystkie zainteresowane strony objęte zakresem tego aktu prawnego. Chociaż koncentrowano się głównie na budowaniu zdolności CSIRT i na platformie umożliwiającej sprawną i skuteczną współpracę operacyjną, wzmacniając tym samym sieć CSIRT, Komisja zbada obecnie, w jaki sposób finansowanie w ramach instrumentu „Łącząc Europę” mogłoby również przynieść korzyści właściwym organom krajowym oraz operatorom usług kluczowych i dostawcom usług cyfrowych.

**Wniosek**

Z uwagi na zbliżający się termin transpozycji dyrektywy w sprawie bezpieczeństwa sieci i informacji do prawa krajowego, który upływa w dniu 9 maja 2018 r., i biorąc pod uwagę termin na zidentyfikowanie operatorów usług kluczowych, który upływa w dniu 9 listopada 2018 r., państwa członkowskie powinny wprowadzić odpowiednie środki w celu zapewnienia, aby przepisy dyrektywy w sprawie bezpieczeństwa sieci i informacji oraz przewidziane w niej modele współpracy mogły zagwarantować jak najlepsze narzędzia na szczeblu UE, które pozwolą osiągnąć wysoki wspólny poziom bezpieczeństwa sieci i systemów informatycznych w całej Unii. Komisja zwraca się do państw członkowskich, aby w ramach tego procesu wzięły pod uwagę stosowne informacje, wytyczne i zalecenia zawarte w niniejszym komunikacie.

Niniejszy komunikat może zostać dodatkowo uzupełniony innymi działaniami, w tym również wynikami trwających prac prowadzonych na forum grupy współpracy.