KOMISJA
EUROPEJSKA

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

ANNEX 1

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

**ZAŁĄCZNIK**

***do***

**KOMUNIKATU 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**

# SPIS TREŚCI

# ZAŁĄCZNIK

## 1. Wprowadzenie

Niniejszy załącznik ma się przyczynić do skutecznego stosowania, wdrożenia i egzekwowania dyrektywy (UE) 2016/1148 w sprawie bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[1] (zwanej dalej „dyrektywą w sprawie bezpieczeństwa sieci i informacji" lub „dyrektywą") oraz pomóc państwom członkowskim w zapewnieniu skutecznego stosowania prawa Unii. Ściślej rzecz biorąc, załącznik ma trzy cele szczegółowe: a) lepsze objaśnienie organom krajowym obowiązków spoczywających na nich na mocy dyrektywy, b) zapewnienie skutecznego egzekwowania przewidzianych w dyrektywie obowiązków spoczywających na podmiotach podlegających wymogom w zakresie bezpieczeństwa i zgłaszania incydentów oraz c) przyczynienie się w wymiarze ogólnym do stworzenia pewności prawa dla wszystkich odpowiednich podmiotów.

Dlatego też niniejszy załącznik zawiera wytyczne dotyczące następujących kwestii o kluczowym znaczeniu dla osiągnięcia celu dyrektywy w sprawie bezpieczeństwa sieci i informacji, tj. zapewnienia wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w UE, który stanowi podstawę funkcjonowania naszego społeczeństwa i gospodarki:

- spoczywającego na państwach członkowskich obowiązku przyjęcia krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych (pkt 2);
- ustanawiania właściwych organów krajowych, pojedynczych punktów kontaktowych i zespołów reagowania na incydenty bezpieczeństwa komputerowego (pkt 3);
- wymogów w zakresie bezpieczeństwa i zgłaszania incydentów mających zastosowanie do operatorów usług kluczowych i dostawców usług cyfrowych (pkt 4); oraz
- związku pomiędzy dyrektywą w sprawie bezpieczeństwa sieci i informacji a innymi aktami prawnymi (pkt 5).

Przy przygotowywaniu niniejszych wytycznych Komisja wykorzystała informacje i dane analityczne zgromadzone podczas opracowywania dyrektywy, a także informacje przekazane przez Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji („ENISA") i grupę współpracy. Komisja oparła się również na doświadczeniach poszczególnych państw członkowskich. W stosownych przypadkach Komisja wzięła pod uwagę zasady przewodnie dokonywania wykładni prawa Unii: brzmienie, kontekst i cele dyrektywy w sprawie bezpieczeństwa sieci i informacji. Z uwagi na fakt, że dyrektywa nie została jeszcze transponowana, Trybunał Sprawiedliwości Unii Europejskiej ani sądy krajowe nie wydały

[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.

jeszcze żadnego orzeczenia w jej sprawie. Dlatego też nie można wykorzystać orzecznictwa jako źródła wytycznych.

Zgromadzenie wszystkich informacji w jednym dokumencie może pozwolić państwom członkowskim na uzyskanie lepszego obrazu dyrektywy, a także na wzięcie tych informacji pod uwagę przy opracowywaniu własnych przepisów krajowych. Jednocześnie Komisja pragnie podkreślić, że niniejszy załącznik nie jest prawnie wiążący, a jego celem nie jest opracowanie nowych przepisów. Nadrzędne kompetencje w zakresie dokonywania wykładni prawa Unii posiada Trybunał Sprawiedliwości Unii Europejskiej.

## 2. Krajowa strategia w zakresie bezpieczeństwa sieci i systemów informatycznych

Zgodnie z art. 7 dyrektywy w sprawie bezpieczeństwa sieci i informacji państwa członkowskie mają obowiązek przyjąć krajową strategię w zakresie bezpieczeństwa sieci i systemów informatycznych, którą będzie można uznać za równoważną krajowej strategii bezpieczeństwa cybernetycznego. Krajowa strategia służy wyznaczeniu celów strategicznych oraz odpowiednich działań w zakresie polityki i działań regulacyjnych w odniesieniu do cyberbezpieczeństwa. Koncepcja krajowej strategii bezpieczeństwa cybernetycznego jest powszechnie stosowana na szczeblu międzynarodowym i w Europie, w szczególności w kontekście współpracy ENISA z państwami członkowskimi nad opracowywaniem krajowych strategii, która niedawno zaowocowała aktualizacją podręcznika dobrych praktyk w zakresie krajowych strategii bezpieczeństwa cybernetycznego[2].

W niniejszym punkcie Komisja wskazuje, w jaki sposób dyrektywa w sprawie bezpieczeństwa sieci i informacji zwiększa gotowość państw członkowskich, zobowiązując je do przyjęcia kompleksowych krajowych strategii w zakresie bezpieczeństwa sieci i systemów informatycznych (art. 7). W punkcie tym odniesiono się do następujących kwestii: a) zakresu strategii oraz b) treści strategii i procedury jej przyjmowania.

Jak zostało to wyjaśnione bardziej szczegółowo poniżej, prawidłowa transpozycja przepisów art. 7 dyrektywy w sprawie bezpieczeństwa sieci i informacji ma zasadnicze znaczenie dla osiągnięcia celów dyrektywy i wymaga przeznaczenia odpowiednich zasobów finansowych i ludzkich na ten cel.

### 2.1. Zakres strategii krajowej

Zgodnie z brzmieniem art. 7 obowiązek przyjęcia krajowej strategii bezpieczeństwa cybernetycznego obejmuje wyłącznie sektory, o których mowa w załączniku II (tj. sektor energetyki, transportu, bankowości, rynków finansowych, służby zdrowia, zaopatrzenia w wodę pitną i jej dystrybucji oraz infrastruktury cyfrowej) i usługi, o których mowa w załączniku III (internetowa platforma handlowa, wyszukiwarka internetowa i usługa przetwarzania w chmurze).

[2] ENISA, *National Cyber-Security Strategy Good Practice* (2016 r.). Dokument dostępny pod adresem: https://www.enisa.europa.eu/publications/ncss-good-practice-guide

W art. 3 dyrektywy w szczególności ustanowiono zasadę harmonizacji minimalnej, zgodnie z którą państwa członkowskie mogą przyjmować lub utrzymywać przepisy mające na celu osiągnięcie wyższego poziomu bezpieczeństwa sieci systemów informatycznych. Zastosowanie tej zasady w odniesieniu do obowiązku przyjęcia „krajowej strategii bezpieczeństwa cybernetycznego" pozwala państwom członkowskim objąć zakresem strategii również sektory i usługi, które nie zostały wymienione w załącznikach II i III do dyrektywy.

W opinii Komisji, a także biorąc pod uwagę cel dyrektywy w sprawie bezpieczeństwa sieci i informacji, tj. osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[3], zalecane byłoby opracowanie strategii krajowej obejmującej wszystkie istotne wymiary społeczeństwa i gospodarki, a nie tylko sektory i usługi cyfrowe wymienione odpowiednio w załącznikach II i III do dyrektywy w sprawie bezpieczeństwa sieci i informacji. Byłoby to zgodne z najlepszymi praktykami międzynarodowymi (zob. wytyczne ITU i analiza OECD przywołane w dalszej części załącznika) oraz z przepisami dyrektywy w sprawie bezpieczeństwa sieci i informacji.

Jak wyjaśniono bardziej szczegółowo poniżej, dotyczy to w szczególności organów administracji publicznej odpowiedzialnych za sektory i usługi inne niż te wymienione w załącznikach II i III do dyrektywy. Administracje publiczne mogą przetwarzać informacje szczególnie chronione, co uzasadnia konieczność objęcia ich krajową strategią bezpieczeństwa cybernetycznego i planami zarządzania zapobiegającymi wyciekom i zapewniającymi odpowiednią ochronę tych informacji.

### 2.2. Treść strategii krajowych i procedura ich przyjmowania

Zgodnie z art. 7 dyrektywy w sprawie bezpieczeństwa sieci i informacji krajowa strategia bezpieczeństwa cybernetycznego musi zawierać przynajmniej następujące elementy:

(i) cele i priorytety krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych;
(ii) ramy zarządzania służące realizacji celów i priorytetów strategii krajowej;
(iii) określenie środków w zakresie gotowości, reagowania i przywracania stanu normalnego, w tym współpracy pomiędzy sektorami publicznym i prywatnym;
(iv) wskazówki odnoszące się do odpowiednich programów edukacyjnych, informacyjnych i szkoleniowych;
(v) wskazówki odnoszące się do planów badawczo-rozwojowych;
(vi) plan oceny ryzyka służący określeniu ryzyk; oraz
(vii) wykaz podmiotów zaangażowanych we wdrażanie strategii.

Ani w art. 7, ani w powiązanym z nim motywie 29 nie określono wymogów, jakie należy spełnić, aby przyjąć krajową strategię bezpieczeństwa cybernetycznego lub aby zwiększyć stopień szczegółowości treści krajowej strategii bezpieczeństwa cybernetycznego. Jeżeli chodzi o procedurę przyjmowania strategii i dodatkowe elementy związane z treścią krajowej strategii bezpieczeństwa cybernetycznego, Komisja uznaje przedstawione poniżej podejście

[3] Zob. art. 1 ust. 1.

za właściwy sposób przyjmowania krajowej strategii bezpieczeństwa cybernetycznego. Wniosek taki opiera się na analizie doświadczeń państw członkowskich i państw trzecich dotyczących sposobu opracowywania przez państwa członkowskie ich własnych strategii. Kolejnym źródłem informacji jest opracowane przez ENISA narzędzie szkoleniowe poświęcone krajowym strategiom bezpieczeństwa cybernetycznego dostępne w formie krótkich filmów i materiałów do pobrania ze strony internetowej ENISA[4].

### 2.3. Procedura i kwestie, które należy poruszyć

Procedura sporządzania i późniejszego przyjmowania strategii krajowej jest złożona i wieloaspektowa, dlatego też zapewnienie jej skuteczności i efektywności wymaga stałego zaangażowania ze strony ekspertów w dziedzinie cyberbezpieczeństwa, przedstawicieli społeczeństwa obywatelskiego i organów odpowiedzialnych za kształtowanie polityki krajowej. W tym kontekście nieodzownym warunkiem jest zapewnienie wsparcia administracyjnego wyższego szczebla co najmniej na poziomie sekretarza stanu lub równoważnym w ministerstwie koordynującym proces realizacji strategii oraz pozyskanie patrona politycznego. Aby pomyślnie przyjąć krajową strategię bezpieczeństwa cybernetycznego, można uwzględnić przedstawioną poniżej pięcioetapową procedurę (zob. wykres 1):

Etap pierwszy – **Ustanowienie zasad przewodnich i wyznaczenie celów strategicznych wynikających ze strategii**

Przede wszystkim właściwe organy krajowe powinny określić pewne kluczowe elementy, które mają znaleźć się w krajowej strategii bezpieczeństwa cybernetycznego, tj. przedstawić pożądane rezultaty, stosując terminologię zgodną z terminologią dyrektywy (art. 7 ust. 1 lit. a) „cele i priorytety"), określić, w jaki sposób rezultaty te będą uzupełniały krajowe polityki społeczne i gospodarcze, oraz ustalić, czy rezultaty te da się pogodzić z przywilejami przysługującymi państwu członkowskiemu Unii Europejskiej i spoczywającymi na nim zobowiązaniami. Cele powinny być skonkretyzowane, mierzalne, osiągalne, realne i terminowe. Można to zilustrować na następującym przykładzie: „Zobowiązujemy się do zagwarantowania, że niniejsza [realizowana w określonych ramach czasowych] strategia będzie bazowała na starannie dobranym, kompleksowym zestawie wskaźników, dzięki którym będziemy w stanie oceniać postępy w dążeniu do uzyskania wyników, które musimy osiągnąć"[5].

Powyższe obejmuje również ocenę polityczną dotyczącą możliwości pozyskania znacznych środków finansowych na cele związane z wdrażaniem strategii. Należy również sporządzić opis planowanego zakresu strategii oraz poszczególnych kategorii zainteresowanych stron z sektora publicznego i prywatnego, które powinny zostać zaangażowane w proces opracowywania poszczególnych celów i działań.

[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool

[5] Cytat z Krajowej strategii bezpieczeństwa cybernetycznego Zjednoczonego Królestwa na lata 2016–2021, s. 67.

Ten pierwszy etap można zrealizować, organizując warsztaty tematyczne z udziałem urzędników ministerialnych wyższego szczebla i polityków moderowane przez ekspertów w dziedzinie cyberbezpieczeństwa dysponujących profesjonalnymi umiejętnościami komunikacyjnymi, którzy są w stanie uwypuklić skutki braku cyberbezpieczeństwa lub niedostatecznego cyberbezpieczeństwa we współczesnej cyfrowej gospodarce i we współczesnym cyfrowym społeczeństwie.

Drugi etap – **Opracowanie treści strategii**

Strategia powinna obejmować środki umożliwiające osiągnięcie wyznaczonych celów, działania przewidziane do realizacji w określonym czasie oraz kluczowe wskaźniki efektywności na potrzeby późniejszej oceny, dopracowywania i udoskonalania strategii po zakończeniu wyznaczonego okresu jej wdrażania. Środki te powinny wspierać wysiłki na rzecz osiągnięcia celu, realizacji priorytetów i uzyskania rezultatów wskazanych jako zasady przewodnie. Wymóg uwzględnienia w strategii środków umożliwiających osiągnięcie wyznaczonych celów został ustanowiony w art. 7 ust. 1 lit. c) dyrektywy w sprawie bezpieczeństwa sieci i informacji.

Zaleca się, aby na potrzeby zarządzania procesem opracowywania strategii i w celu ułatwienia przekazywania stosownych informacji powołać grupę sterującą pod przewodnictwem ministerstwa koordynującego proces wdrażania strategii. Można to osiągnąć, powołując szereg grup redakcyjnych zrzeszających odpowiednich urzędników i ekspertów wokół najważniejszych ogólnych zagadnień, takich jak np. ocena ryzyka, planowanie ewentualnościowe, zarządzanie incydentami, rozwijanie umiejętności, podnoszenie świadomości, badania i rozwój przemysłowy itp. Każdy sektor z osobna (np. sektor energetyki, transportu itp.) zostałby również poproszony o ocenę skutków jego objęcia strategią, w tym również związanych z pozyskaniem koniecznych zasobów, oraz o zaangażowanie wyznaczonych operatorów usług kluczowych i dostawców kluczowych usług cyfrowych w ustalanie priorytetów i składanie wniosków na potrzeby procesu opracowywania strategii. Zaangażowanie zainteresowanych stron z poszczególnych sektorów ma zasadnicze znaczenie również z uwagi na konieczność zapewnienia zharmonizowanego wdrażania dyrektywy w poszczególnych sektorach przy jednoczesnym należytym uwzględnieniu ich specyfiki.

Trzeci etap – **Opracowanie ram zarządzania**

Aby ramy zarządzania były wydajne i skuteczne, powinny opierać się na kluczowych zainteresowanych stronach, priorytetach wyznaczonych w procesie ich opracowywania oraz ograniczeniach i kontekście krajowych struktur administracyjnych i politycznych. Wskazane byłoby bezpośrednie składanie sprawozdań na szczeblu politycznym, wyposażenie ram w zdolności do podejmowania decyzji i przydziału zasobów, a także przekazywanie informacji od specjalistów w dziedzinie cyberbezpieczeństwa i zainteresowanych stron z poszczególnych sektorów. W art. 7 ust. 1 lit. b) dyrektywy w sprawie bezpieczeństwa sieci i informacji odniesiono się do ram zarządzania i wyraźnie wskazano „zakresy obowiązków organów rządowych i innych właściwych podmiotów”.

Czwarty etap – **Sporządzenie projektu strategii i dokonanie jego przeglądu**

Na tym etapie projekt strategii powinien zostać sporządzony i poddany przeglądowi przy wykorzystaniu analizy mocnych i słabych stron oraz szans i zagrożeń (SWOT), której wyniki mogą ułatwić podjęcie decyzji w kwestii tego, czy w treści strategii należy wprowadzić zmiany. Po zakończeniu wewnętrznego przeglądu powinny się odbyć konsultacje z zainteresowanymi stronami. W tym kontekście należałoby również przeprowadzić konsultacje publiczne, aby uzmysłowić opinii publicznej znaczenie proponowanej strategii, zebrać informacje ze wszystkich możliwych źródeł i zwrócić się o wsparcie w pozyskaniu zasobów niezbędnych do późniejszego wdrożenia strategii.

Piąty etap – **Oficjalne przyjęcie**

Ten ostatni etap obejmuje oficjalne przyjęcie strategii na szczeblu politycznym i uchwalenie budżetu na jej realizację, który odzwierciedla znaczenie, jakie dane państwo członkowskie przywiązuje do kwestii cyberbezpieczeństwa. Aby osiągnąć cele dyrektywy w sprawie bezpieczeństwa sieci i informacji, Komisja zachęca państwa członkowskie do przekazywania informacji na temat budżetu przy przedkładaniu Komisji dokumentu zawierającego strategię krajową zgodnie z art. 7 ust. 3 dyrektywy. Podjęcie zobowiązań dotyczących budżetu i niezbędnych zasobów ludzkich ma absolutnie kluczowe znaczenie dla skutecznego wdrażania strategii i dyrektywy. 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.

Porady dotyczące procedury przyjmowania strategii krajowych i treści tych strategii udostępniane przez różne źródła publiczne i akademickie – na przykład przez ENISA[6], ITU[7], OECD[8], Globalne Forum Wiedzy Cyfrowej oraz Uniwersytet Oksfordzki[9].

[6] ENISA, *National Cyber-Security Strategy Good Practice* (2016 r.). Dokument dostępny pod adresem: https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[7] ITU, *National Cybersecurity Strategy Guide* (2011 r.). Dokument dostępny pod adresem: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf
ITU opublikuje również w 2017 r. zestaw narzędzi dotyczących krajowej strategii bezpieczeństwa cybernetycznego (zob. prezentacja dostępna pod adresem http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf).

[8] OECD, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies* (2012 r.). Dokument dostępny pod adresem: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

[9] Globalne Centrum Zdolności w obszarze Cyberbezpieczeństwa i Uniwersytet Oksfordzki, *Global Cybersecurity Capacity Maturity Model for Nations (CMM) – wydanie zmienione* (2016 r.). Dokument dostępny pod adresem: https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf

## 2.4. Konkretne działania, jakie państwa członkowskie muszą podjąć przed upływem terminu transpozycji

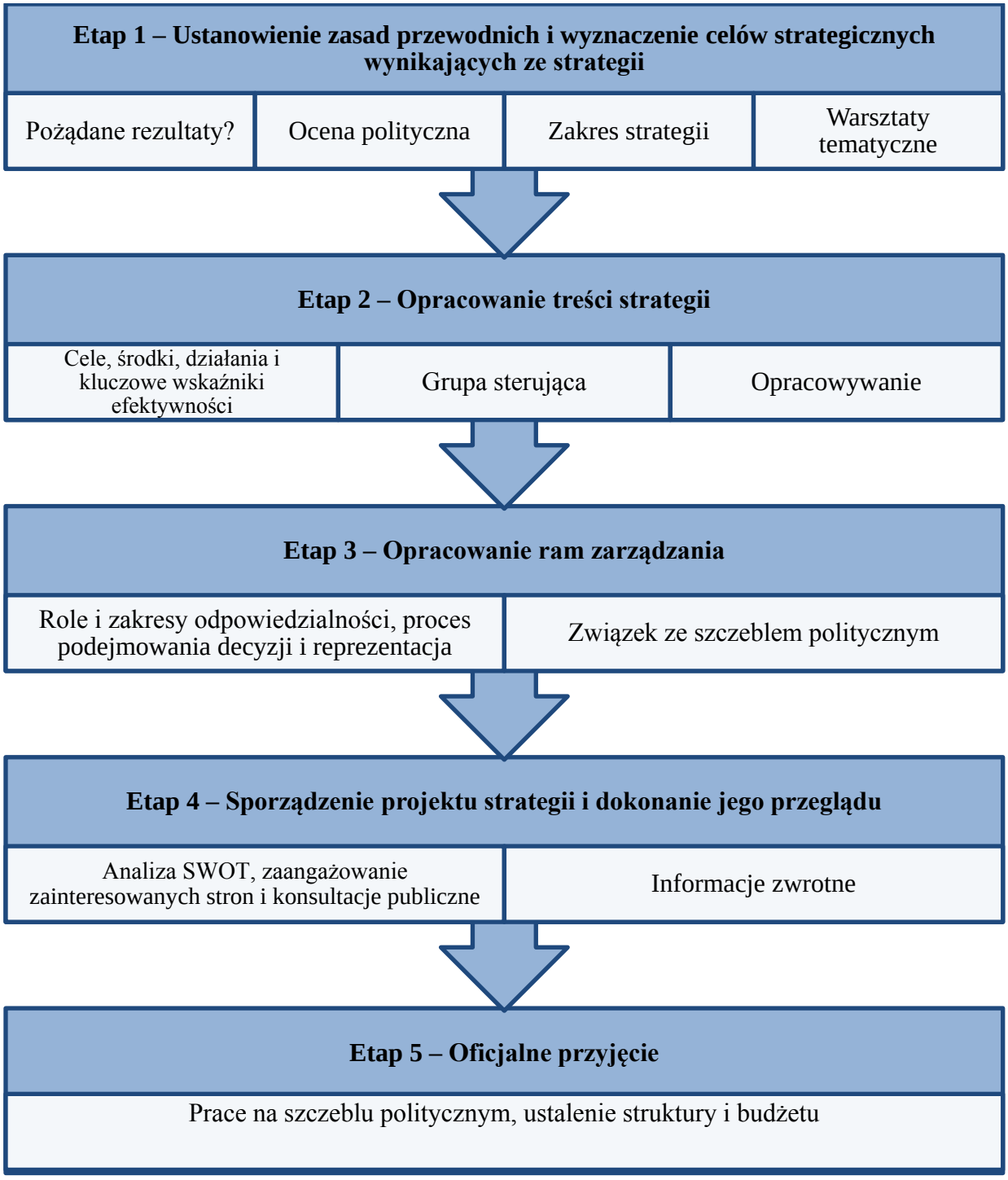
Przed przyjęciem dyrektywy niemal wszystkie państwa członkowskie[10] opublikowały już dokumenty oznaczone jako krajowe strategie bezpieczeństwa cybernetycznego. W pkt 6 niniejszego załącznika wymieniono strategie aktualnie obowiązujące w poszczególnych państwach członkowskich[11]. Strategie zawierają zazwyczaj zasady strategiczne, wytyczne, cele, a w niektórych przypadkach również szczególne środki służące przeciwdziałaniu zagrożeniom dla cyberbezpieczeństwa.

Biorąc pod uwagę fakt, że niektóre z tych strategii zostały przyjęte przed przyjęciem dyrektywy w sprawie bezpieczeństwa sieci i informacji, strategie te niekoniecznie muszą zawierać wszystkie elementy wymienione w art. 7. Aby zapewnić prawidłową transpozycję dyrektywy, państwa członkowskie będą musiały przeprowadzić analizę luk, badając treść krajowych strategii bezpieczeństwa cybernetycznego pod kątem siedmiu odrębnych wymogów wymienionych w art. 7 w odniesieniu do wszystkich sektorów wymienionych w załączniku II do dyrektywy i wszystkich usług wymienionych w załączniku III do dyrektywy. Państwa członkowskie będą mogły następnie wyeliminować zidentyfikowane luki, dokonując zmiany swoich istniejących krajowych strategii bezpieczeństwa cybernetycznego albo przeprowadzając pełny przegląd zasad stanowiących fundament ich krajowej strategii bezpieczeństwa sieci i informacji i opracowując tę strategię od podstaw. Przedstawione powyżej wytyczne dotyczące procedury przyjmowania krajowej strategii bezpieczeństwa cybernetycznego są również istotne w kontekście przeglądu i aktualizacji istniejących krajowych strategii bezpieczeństwa cybernetycznego.

[10] Poza Grecją, gdzie krajowa strategia bezpieczeństwa cybernetycznego jest przygotowywana od 2014 r. (zob. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view).

[11] Informacje te pochodzą z przeglądu krajowych strategii bezpieczeństwa cybernetycznego opublikowanego przez ENISA pod adresem https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

**Wykres 1: Pięcioetapowy proces przyjmowania krajowej strategii bezpieczeństwa cybernetycznego**




### 3. Dyrektywa w sprawie bezpieczeństwa sieci i informacji: właściwe organy krajowe, pojedyncze punkty kontaktowe i zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT)

Zgodnie z art. 8 ust. 1 państwa członkowskie są zobowiązane do wyznaczenia jednego właściwego organu krajowego lub większej liczby takich organów obejmujących co najmniej

sektory, o których mowa w załączniku II do dyrektywy, i usługi, o których mowa w załączniku III do dyrektywy, i powierzenia tym organom zadania monitorowania procesu stosowania dyrektywy. Państwa członkowskie mogą do tej roli wyznaczyć istniejący organ lub istniejące organy.

W niniejszym punkcie skoncentrowano się na sposobach zwiększenia przez dyrektywę w sprawie bezpieczeństwa sieci i informacji gotowości państw członkowskich poprzez wprowadzenie wymogu posiadania efektywnych właściwych organów krajowych i zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT). Ściślej rzecz biorąc, niniejszy punkt dotyczy obowiązku wyznaczenia właściwych organów krajowych oraz roli pojedynczego punktu kontaktowego. Omówiono w nim trzy zagadnienia: a) możliwe krajowe struktury zarządzania (np. modele scentralizowane, zdecentralizowane itp.) i inne wymogi; b) rolę pojedynczego punktu kontaktowego oraz c) zespoły reagowania na incydenty bezpieczeństwa komputerowego.

### 3.1. Rodzaje organów

Zgodnie z art. 8 dyrektywy w sprawie bezpieczeństwa sieci i informacji państwa członkowskie są zobowiązane do wyznaczenia właściwych organów krajowych ds. bezpieczeństwa sieci i systemów informatycznych, przy czym w artykule tym wprost przewidziano możliwość wyznaczenia „jednego lub większej liczby właściwych organów krajowych". W motywie 30 dyrektywy wyjaśniono ten wybór polityczny: „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".

Państwa członkowskie mogą zatem wyznaczyć jeden centralny organ zajmujący się wszystkimi sektorami i usługami objętymi przepisami dyrektywy lub szereg organów, np. w zależności od rodzaju sektora.

Przy wyborze odpowiedniego podejścia państwa członkowskie mogą oprzeć się na doświadczeniu zyskanym w ramach podejść krajowych wykorzystywanych w kontekście istniejących przepisów w zakresie ochrony krytycznej infrastruktury teleinformatycznej. Jak opisano w tabeli 1, przy przydzielaniu zadań na szczeblu krajowym w zakresie ochrony krytycznej infrastruktury teleinformatycznej państwa członkowskie zastosowały podejście scentralizowane albo zdecentralizowane. Przedstawione w tym punkcie przykłady krajowe mają wyłącznie charakter poglądowy i służą zwróceniu uwagi państw członkowskich na istniejące ramy organizacyjne. Dlatego też Komisja nie sugeruje, że model zastosowany przez poszczególne państwa do celów związanych z ochroną krytycznej infrastruktury teleinformatycznej powinien zostać koniecznie zastosowany przy transpozycji dyrektywy w sprawie bezpieczeństwa sieci i informacji.

Państwa członkowskie mogą również zdecydować się na różnego rodzaju rozwiązania hybrydowe, łączące elementy zarówno podejścia scentralizowanego, jak i zdecentralizowanego. Wyborów można dokonywać zgodnie z wcześniejszymi krajowymi rozwiązaniami w obszarze zarządzania przyjętymi dla poszczególnych sektorów i usług objętych przepisami dyrektywy lub na podstawie nowych rozwiązań określonych przez właściwe organy i odpowiednie zainteresowane strony zidentyfikowane jako operatorzy usług kluczowych i dostawcy usług cyfrowych. Istotnymi czynnikami wpływającymi na wybory podejmowane przez państwa członkowskie mogą być również istniejące zasoby wiedzy specjalistycznej w zakresie cyberbezpieczeństwa, kwestie związane z pozyskiwaniem zasobów i relacje między zainteresowanymi stronami a interesem narodowym (na przykład w obszarze rozwoju gospodarczego, bezpieczeństwa publicznego itp.).

### 3.2. Informowanie i dodatkowe istotne kwestie

Zgodnie z art. 8 ust. 7 państwa członkowskie muszą powiadomić Komisję o wyznaczeniu właściwych organów krajowych oraz o ich zadaniach. Stosowne informacje należy przekazać przed upływem terminu transpozycji.

Zgodnie z art. 15 i 17 dyrektywy w sprawie bezpieczeństwa sieci i informacji państwa członkowskie są zobowiązane do zapewnienia, aby właściwe organy dysponowały określonymi uprawnieniami i środkami niezbędnymi do wykonywania zadań, o których mowa w tych artykułach.

Ponadto informacje o wyznaczeniu określonych podmiotów jako właściwych organów krajowych muszą zostać podane do wiadomości publicznej. Dyrektywa nie precyzuje, w jaki sposób należy informować społeczeństwo. Zważywszy na fakt, że celem tego wymogu jest osiągnięcie wysokiego poziomu świadomości wśród podmiotów podlegających przepisom w zakresie bezpieczeństwa sieci i informacji i ogółu społeczeństwa, oraz w oparciu o doświadczenia zgromadzone w innych sektorach (sektorze telekomunikacji, sektorze bankowym, sektorze produktów leczniczych) Komisja uważa, że wymóg ten można spełnić na przykład poprzez utworzenie odpowiednio rozreklamowanego portalu.

Zgodnie z art. 8 ust. 5 dyrektywy w sprawie bezpieczeństwa sieci i informacji tego rodzaju organy muszą dysponować „odpowiednimi zasobami” umożliwiającymi im wykonywanie zadań powierzonych na mocy dyrektywy.

**Tabela 1: Krajowe podejścia do ochrony krytycznej infrastruktury teleinformatycznej**

W 2016 r. ENISA opublikowała badanie[12] dotyczące różnych podejść poszczególnych państw członkowskich do zapewnienia należytej ochrony ich krytycznych infrastruktur teleinformatycznych. W badaniu opisano dwa profile zarządzania ochroną krytycznej infrastruktury teleinformatycznej w państwach członkowskich, które można wykorzystać w kontekście transpozycji dyrektywy w sprawie bezpieczeństwa sieci i informacji.

**Profil 1: Podejście zdecentralizowane, w ramach którego wiele organów sektorowych pełni funkcję organów właściwych w odniesieniu do konkretnych sektorów i usług, o których mowa w załącznikach II i III do dyrektywy**

Cechy podejścia zdecentralizowanego:

(i) stosowanie zasady pomocniczości;
(ii) ścisła współpraca między agencjami publicznymi;
(iii)stosowanie przepisów sektorowych.

*Stosowanie zasady pomocniczości*

Zamiast powoływać lub wyznaczać jedną agencją ponoszącą ogólną odpowiedzialność za podejmowanie działań w tym obszarze, w ramach podejścia zdecentralizowanego stosuje się zasadę pomocniczości. Oznacza to, że odpowiedzialność za wdrożenie strategii spoczywa na organie sektorowym, który najlepiej rozumie specyfikę lokalnego sektora i który utrzymuje nawiązane wcześniej relacje z zainteresowanymi stronami. Zgodnie z tą zasadą decyzje podejmują organy znajdujące się najbliżej podmiotów, na które decyzje te wywierają wpływ.

*Ścisła współpraca między agencjami publicznymi*

Z uwagi na różnorodność agencji publicznych zaangażowanych w ochronę krytycznej infrastruktury teleinformatycznej wiele państw członkowskich opracowało programy współpracy w celu skoordynowania działań i wysiłków podejmowanych przez poszczególne organy. Wspomniane programy współpracy mogą mieć formę nieformalnych sieci albo bardziej zinstytucjonalizowanych forów lub rozwiązań. Celem tych programów współpracy jest jednak wyłącznie wymiana informacji i koordynowanie działań podejmowanych przez poszczególne agencje publiczne – podmioty zaangażowane w realizację tych programów nie mają żadnych uprawnień w odniesieniu do agencji publicznych.

*Stosowanie przepisów sektorowych*

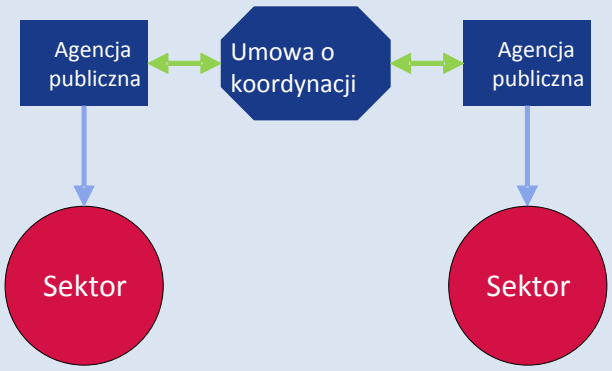
Państwa stosujące podejście zdecentralizowane w odniesieniu do sektorów krytycznych często rezygnują z przyjmowania przepisów do celów związanych z ochroną krytycznej infrastruktury teleinformatycznej. Zamiast tego przyjmują sektorowe przepisy i regulacje, które mogą się znacznie różnić w poszczególnych sektorach. Zastosowanie tego podejścia przyniosłoby

[12] ENISA, *Stocktaking, Analysis and Recommendations on the protection of CIIs* (2016 r.). Dokument dostępny pod adresem: https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

korzyści w postaci dostosowania środków powiązanych z bezpieczeństwem sieci i informacji do istniejących regulacji sektorowych w celu zwiększenia poziomu akceptacji dla tego rodzaju środków wśród przedstawicieli sektora i poprawy skuteczności egzekwowania przepisów przez właściwy organ.

Zastosowanie czysto zdecentralizowanego podejścia wiąże się ze znacznym ryzykiem wystąpienia niespójności w stosowaniu przepisów dyrektywy w odniesieniu do różnych sektorów i usług. W takim przypadku dyrektywa przewiduje krajowy pojedynczy punkt kontaktowy pełniący funkcję łącznikową w kwestiach transgranicznych – dane państwo członkowskie może powierzyć również temu podmiotowi zadanie wewnętrznego koordynowania działań między wieloma właściwymi organami krajowymi i nadzorowania współpracy między tymi organami prowadzonej zgodnie z art. 10 dyrektywy.

**Wykres 2: Podejście zdecentralizowane**




*Przykłady państw stosujących podejście zdecentralizowane*

Szwecja to dobry przykład państwa stosującego podejście zdecentralizowane w kwestiach związanych z ochroną krytycznej infrastruktury teleinformatycznej. W państwie tym stosuje się „perspektywę systemową", co oznacza, że odpowiedzialność za wykonywanie głównych zadań w obszarze ochrony krytycznej infrastruktury teleinformatycznej, takich jak identyfikowanie usług kluczowych i infrastruktur krytycznych, koordynowanie działań operatorów i udzielanie im wsparcia, wykonywanie zadań regulacyjnych oraz stosowanie środków w obszarze gotowości na wypadek sytuacji wyjątkowej spoczywa na różnych agencjach i gminach. Wśród tych agencji należy wymienić Szwedzką Agencję ds. Cywilnych Planów Awaryjnych (MSB), Szwedzką Agencję Poczty i Telekomunikacji (PTS) oraz szereg szwedzkich agencji prowadzących działalność w sektorze obronności, wojskowości i egzekwowania prawa.

Aby skoordynować działania podejmowane przez poszczególne agencje i podmioty publiczne, rząd szwedzki opracował sieć współpracy zrzeszającą organy „o określonych obowiązkach w zakresie bezpieczeństwa informacji społecznych". W skład wspomnianej sieci, której oficjalna nazwa to grupa współpracy na rzecz bezpieczeństwa informacji (SAMFI), wchodzą

przedstawiciele poszczególnych organów; członkowie grupy spotykają się kilka razy w roku w celu omówienia kwestii istotnych z punktu widzenia bezpieczeństwa informacji na szczeblu krajowym. Przedmiotem zainteresowania SAMFI są głównie kwestie o charakterze polityczno-strategicznym i zagadnienia takie jak problematyka techniczna i normalizacyjna, rozwój w dziedzinie bezpieczeństwa informacji na szczeblu krajowym i międzynarodowym lub zarządzanie incydentami informatycznymi i zapobieganie takim incydentom. (Szwedzka Agencja ds. Cywilnych Planów Awaryjnych (MSB), 2015 r.).

Szwecja nie przyjęła ustawy ogólnej regulującej kwestie związane z ochroną krytycznej infrastruktury teleinformatycznej, która miałaby zastosowanie do operatorów krytycznej infrastruktury teleinformatycznej we wszystkich sektorach. Zamiast tego odpowiedzialność za przyjmowanie przepisów nakładających stosowne obowiązki na przedsiębiorstwa w konkretnych sektorach spoczywa na właściwych organach publicznych. Na przykład MSB jest uprawniona do wydawania wiążących dla organów rządowych przepisów w obszarze bezpieczeństwa informacji, natomiast PTS może zobowiązać operatorów do wdrożenia określonych technicznych lub organizacyjnych środków bezpieczeństwa na podstawie przepisów prawa wtórnego.

Innym przykładem państwa wykazującego cechy typowe dla tego profilu jest Irlandia. Irlandia stosuje „doktrynę pomocniczości", zgodnie z którą każde ministerstwo jest odpowiedzialne za identyfikowanie krytycznej infrastruktury teleinformatycznej i przeprowadzanie oceny ryzyka w swoim sektorze. Ponadto na szczeblu krajowym nie przyjęto żadnych konkretnych regulacji w zakresie ochrony krytycznej infrastruktury teleinformatycznej. Przepisy mają charakter sektorowy i dotyczą głównie sektora energetyki i telekomunikacji (2015 r.). Inne przykłady to Austria, Cypr i Finlandia.

**Profil 2: Podejście scentralizowane, w ramach którego jeden organ na szczeblu centralnym jest odpowiedzialny za wszystkie sektory i usług, o których mowa w załącznikach II i III do dyrektywy**

Cechy podejścia scentralizowanego:

(i) organ centralny odpowiedzialny za wszystkie sektory;
(ii) kompleksowe przepisy.

*Organ centralny odpowiedzialny za wszystkie sektory*

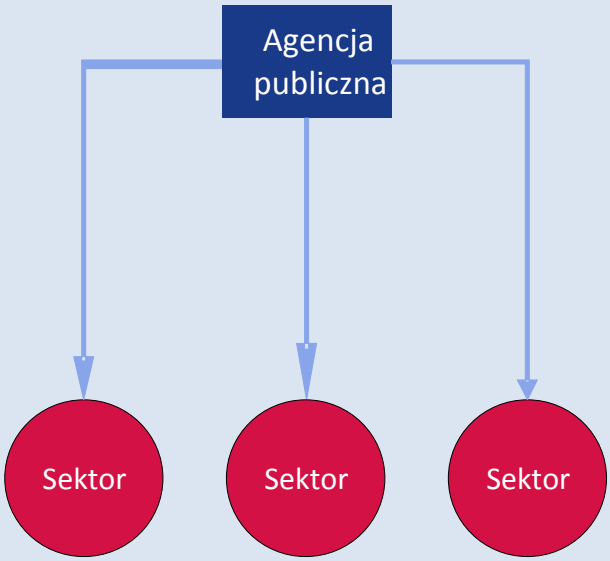
Państwa członkowskie stosujące podejście scentralizowane ustanowiły organy realizujące zadania i dysponujące szerokimi uprawnieniami w szeregu lub we wszystkich sektorach krytycznych lub rozszerzyły uprawnienia przysługujące istniejącym organom. Główne organy odpowiedzialne za ochronę krytycznej infrastruktury teleinformatycznej podejmują szereg różnych zadań jednocześnie – wśród tych zadań należy wymienić planowanie ewentualnościowe, zarządzanie sytuacjami wyjątkowymi, zadania regulacyjne i wspieranie operatorów prywatnych. W wielu przypadkach krajowy lub rządowy CSIRT wchodzi w skład głównego organu odpowiedzialnego za ochronę krytycznej infrastruktury teleinformatycznej. Organ centralny dysponuje zazwyczaj większymi zasobami wiedzy fachowej w dziedzinie

cyberbezpieczeństwa niż szereg organów sektorowych, biorąc pod uwagę ogólny niedobór umiejętności w zakresie cyberbezpieczeństwa.

*Kompleksowe przepisy*

Kompleksowe przepisy nakładają obowiązki i wymogi na wszystkich operatorów krytycznej infrastruktury teleinformatycznej we wszystkich sektorach. Cel ten można osiągnąć, przyjmując nowe, kompleksowe przepisy lub uzupełniając już istniejące przepisy sektorowe. Stosowanie tego podejścia przyczyniłoby się do spójnego stosowania przepisów dyrektywy w sprawie bezpieczeństwa sieci i informacji w odniesieniu do wszystkich sektorów i usług objętych jej zakresem. Podejście to pozwoliłoby wyeliminować ryzyko wystąpienia niespójności w procesie wdrażania dyrektywy, które mogłoby wystąpić w przypadku wyznaczenia szeregu organów o określonych uprawnieniach.

**Wykres 3: Podejście scentralizowane**



*Przykłady państw stosujących podejście scentralizowane*

Francja to dobry przykład państwa członkowskiego UE stosującego podejście scentralizowane. W 2011 r. Francuska Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) została wyznaczona jako główny organ krajowy odpowiedzialny za ochronę systemów informatycznych. ANSSI pełni ważną funkcję nadzorczą w odniesieniu do „operatorów o kluczowym znaczeniu" (OIV): agencja może im nakazać, aby dostosowali się do środków bezpieczeństwa, i jest uprawniona do poddawania ich audytom bezpieczeństwa. Ponadto agencja pełni funkcję głównego pojedynczego punktu kontaktowego dla OIV, które są zobowiązane do zgłaszania jej incydentów bezpieczeństwa.

Jeżeli chodzi o incydenty bezpieczeństwa, ANSSI pełni funkcję agencji odpowiedzialnej za podejmowanie działań w sytuacjach nadzwyczajnych w celu zapewnienia ochrony krytycznej infrastruktury teleinformatycznej oraz za wskazywanie środków, jakie operatorzy muszą wprowadzać w odpowiedzi na sytuację kryzysową. Rząd koordynuje swoje działania z centrum operacyjnym ANSSI. Odpowiedzialność za wykrywanie zagrożeń i reagowanie na incydenty na szczeblu operacyjnym spoczywa na CERT-FR, które wchodzi w skład ANSSI.

Francja ustanowiła kompleksowe ramy prawne w zakresie ochrony krytycznej infrastruktury teleinformatycznej. W 2006 r. premier nakazał sporządzenie listy sektorów o istotnym znaczeniu dla infrastruktury krytycznej. Na podstawie tej listy, na której figurowało dwanaście kluczowych sektorów, rząd zidentyfikował około 250 OIV. W 2013 r. promulgowano ustawę o programowaniu do celów wojskowych[13]. W ustawie tej na OIV nałożono różne obowiązki, m.in. obowiązek zgłaszania incydentów lub obowiązek wdrażania środków bezpieczeństwa. Wymogi ustanowione w ustawie obowiązują wszystkie OIV we wszystkich sektorach (francuski senat, 2013 r.).

### 3.3. Dyrektywa w sprawie bezpieczeństwa sieci i informacji, art. 9: Zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT)

Zgodnie z art. 9 państwa członkowskie są zobowiązane do wyznaczenia jednego CSIRT lub większej ich liczby i powierzenia im zadania radzenia sobie z zagrożeniami i incydentami związanymi z sektorami wymienionymi w załączniku II do dyrektywy w sprawie bezpieczeństwa sieci i informacji i usługami wymienionymi w załączniku III do tej dyrektywy. Biorąc pod uwagę wymóg dotyczący harmonizacji minimalnej przewidziany w art. 3 tej dyrektywy, państwa członkowskie dysponują swobodą uznania w kwestii wykorzystywania CSIRT również w innych sektorach nieobjętych przepisami dyrektywy, takich jak sektor administracji publicznej.

[13] La loi de programmation militaire.

Państwa członkowskie mogą ustanowić CSIRT w ramach właściwego organu krajowego[14].

### 3.4. Zadania i wymogi

Zadania wyznaczonych CSIRT, określone w załączniku I do dyrektywy w sprawie bezpieczeństwa sieci i informacji, obejmują:

- monitorowanie incydentów na poziomie krajowym;
- przekazywanie zainteresowanym stronom wczesnych ostrzeżeń, ogłaszania alarmów, wydawania ogłoszeń i przekazywania skierowanych do zainteresowanych stron informacji dotyczących ryzyk i incydentów;
- reagowanie na incydenty;
- zapewnianie dynamicznej analizy ryzyka i incydentów oraz orientacji sytuacyjnej; oraz
- udział w sieci krajowych CSIRT (sieci CSIRT) ustanowionej na mocy art. 12.

W art. 14 ust. 3, 5 i 6 oraz w art. 16 ust. 3, 6 i 7 określono określone dodatkowe zadania związane ze zgłaszaniem incydentów, które CSIRT mogą wykonywać, jeżeli państwo członkowskie zdecyduje się powierzyć im odpowiedzialność za ich wykonywanie niezależnie od właściwych organów krajowych lub w zastępstwie tych organów.

W trakcie transpozycji dyrektywy państwa członkowskie mogą skorzystać z wariantów przy określaniu roli CSIRT w odniesieniu do wymogów dotyczących zgłaszania incydentów. Można wprowadzić wymóg obowiązkowego bezpośredniego przekazywania informacji CSIRT, co przyniosłoby korzyści w postaci wydajności administracyjnej, lub przyjąć rozwiązanie przewidujące bezpośrednie przekazywanie informacji właściwym organom krajowym i udzielenie CSIRT prawa dostępu do przekazanych informacji. Głównym przedmiotem zainteresowania CSIRT jest rozwiązywanie problemów napotykanych przez ich zainteresowane strony w kwestiach związanych z powstrzymywaniem i wykrywaniem incydentów cybernetycznych, reagowaniem na nie i łagodzeniem ich skutków (uwzględniając incydenty niepodlegające obowiązkowemu zgłoszeniu), natomiast odpowiedzialność za przestrzeganie uregulowań spoczywa na właściwych organach krajowych.

Zgodnie z art. 9 ust. 3 dyrektywy państwa członkowskie muszą również zapewnić, aby takie CSIRT miały dostęp do bezpiecznej i odpornej infrastruktury ICT.

Zgodnie z art. 9 ust. 4 dyrektywy państwa członkowskie są zobowiązane do przekazywania Komisji informacji o zakresie kompetencji wyznaczonych CSIRT i o głównych elementach procedur postępowania w przypadku incydentu.

W załączniku I do dyrektywy w sprawie bezpieczeństwa sieci i informacji przedstawiono wymogi spoczywające na CSIRT wyznaczonych przez państwa członkowskie. CSIRT jest zobowiązany do zapewnienia wysokiego poziomu dostępności swoich usług komunikacyjnych. Pomieszczenia CSIRT oraz wspierające systemy informatyczne muszą być

[14] Zob. art. 9 ust. 1 zdanie ostatnie.

zlokalizowane w bezpiecznych miejscach i być odpowiednie do zapewnienia ciągłości działania. Ponadto CSIRT powinien mieć możliwość udziału w międzynarodowych sieciach współpracy.

### 3.5. Wsparcie w zakresie rozwoju CSIRT

Program infrastruktury usług cyfrowych (DSI) w zakresie bezpieczeństwa cybernetycznego w ramach instrumentu „Łącząc Europę" może stanowić źródło znacznych środków unijnych na wspieranie CSIRT państw członkowskich w dążeniu do zwiększania ich zdolności i usprawniania wzajemnej współpracy za pośrednictwem mechanizmu współpracy w zakresie wymiany informacji. Celem mechanizmu współpracy opracowywanego w ramach projektu SMART 2015/1089 jest usprawnienie szybkiej i skutecznej współpracy operacyjnej prowadzonej na zasadzie dobrowolności między CSIRT państw członkowskich, głównie w celu udzielenia wsparcia przy realizacji zadań powierzonych sieci CSIRT zgodnie z art. 12 dyrektywy.

Szczegółowe informacje na temat odpowiednich zaproszeń do składania wniosków dotyczących budowania zdolności CSIRT państw członkowskich można uzyskać, odwiedzając stronę internetową Agencji Wykonawczej ds. Innowacyjności i Sieci Komisji Europejskiej[15].

Rada zarządzająca programu infrastruktur usług cyfrowych na rzecz cyberbezpieczeństwa w ramach instrumentu „Łącząc Europę" zapewnia nieformalną strukturę umożliwiającą dostarczanie CSIRT państw członkowskich wytycznych i udzielanie im wsparcia na szczeblu politycznym w celu budowania zdolności oraz wdrażania dobrowolnego mechanizmu współpracy.

Nowo utworzony CSIRT lub CSIRT wyznaczony do pełnienia zadań, o których mowa w załączniku I do dyrektywy w sprawie bezpieczeństwa sieci i informacji, może korzystać z porad i wiedzy fachowej ENISA w celu poprawy swoich wyników i skutecznego wywiązywania się z powierzonych mu zadań[16]. W tym względzie warto podkreślić, że CSIRT państw członkowskich mogłyby wykorzystać jako punkt odniesienia wyniki prac przeprowadzonych niedawno przez ENISA. W szczególności – jak wskazano w pkt 7 niniejszego załącznika – Agencja opublikowała szereg dokumentów i opracowań zawierających wyniki badań, w których opisano dobre praktyki i zalecenia na szczeblu technicznym obejmujące oceny stopnia dojrzałości CSIRT w odniesieniu do poszczególnych zdolności CSIRT i świadczonych przez nie usług. Ponadto wytyczne i najlepsze praktyki były również przedmiotem wymiany w ramach sieci CSIRT zarówno na szczeblu globalnym (FIRST[17]), jak i na szczeblu europejskim (inicjatywa Trusted Introducer, TI[18]).

[15] Dostępną pod adresem: https://ec.europa.eu/inea/en/connecting-europe-facility
[16] Zob. art. 9 ust. 5 dyrektywy w sprawie bezpieczeństwa sieci i informacji.
[17] Forum Zespołów Reagowania na Incydenty Bezpieczeństwa (https://www.first.org/).
[18] https://www.trusted-introducer.org/

### 3.6. Rola pojedynczego punktu kontaktowego

Zgodnie z art. 8 ust. 3 dyrektywy w sprawie bezpieczeństwa sieci i informacji każde państwo członkowskie musi wyznaczyć krajowy pojedynczy punkt kontaktowy, który będzie pełnił funkcję łącznikową w celu zapewnienia transgranicznej współpracy z odpowiednimi organami w innych państwach członkowskich, a także z grupą współpracy i siecią CSIRT[19] powołaną na mocy samej dyrektywy. W motywie 31 i w art. 8 ust. 4 dyrektywy przedstawiono uzasadnienie tego wymogu – jego ustanowienie służy usprawnieniu transgranicznej współpracy i wymiany informacji. Jest to konieczne w szczególności z uwagi na fakt, że państwa członkowskie mogą wyznaczyć więcej niż jeden organ krajowy. Wyznaczenie pojedynczego punktu kontaktowego wniosłoby zatem wkład w proces identyfikacji organów z poszczególnych państw członkowskich i rozwijania współpracy między tymi organami.

W przypadkach, gdy krajowy pojedynczy punkt kontaktowy nie jest CSIRT ani członkiem grupy współpracy, funkcja łącznikowa pojedynczego punktu kontaktowego sprowadza się zazwyczaj do utrzymywania kontaktów z sekretariatami grupy współpracy i sieci CSIRT. Ponadto państwa członkowskie muszą zapewnić informowanie pojedynczego punktu kontaktowego o zgłoszeniach otrzymywanych od operatorów usług kluczowych i dostawców usług cyfrowych[20].

Art. 8 ust. 3 dyrektywy stanowi, że w przypadku, gdy państwo członkowskie przyjęło podejście scentralizowane, tj. wyznaczyło tylko jeden właściwy organ, taki organ będzie pełnił również funkcję pojedynczego punktu kontaktowego. Jeżeli państwo członkowskie zdecydowało się zastosować podejście zdecentralizowane, może powierzyć pełnienie funkcji pojedynczego punktu kontaktowego jednemu z wyznaczonych przez siebie właściwych organów. Niezależnie od wybranego modelu instytucjonalnego, we wszystkich przypadkach, w których właściwy organ, CSIRT i pojedynczy punkt kontaktowy są różnymi organami, państwa członkowskie są zobowiązane do zapewnienia skutecznej współpracy między nimi w celu spełnienia wymogów przewidzianych w dyrektywie[21].

W terminie do dnia 9 sierpnia 2018 r., a następnie raz do roku pojedynczy punkt kontaktowy jest zobowiązany do przekazania grupie współpracy sprawozdania podsumowującego na temat otrzymanych zgłoszeń, które zawiera informacje o liczbie zgłoszeń, charakterze zgłoszonych incydentów i działaniach podjętych przez organy, takich jak informowanie o incydencie innych państw członkowskich, na które wywarł on wpływ, lub przekazywanie przedsiębiorstwu zgłaszającemu stosownych informacji dotyczących sposobu radzenia sobie z incydentem[22]. Na wniosek właściwego organu lub CSIRT pojedynczy punkt kontaktowy

[19] Sieć krajowych CSIRT utworzona na mocy art. 12 do celów współpracy operacyjnej między państwami członkowskimi.
[20] Zob. art. 10 ust. 3.
[21] Zob. art. 10 ust. 1.
[22] Tamże.

jest zobowiązany do przekazania zgłoszeń operatorów usług kluczowych pojedynczym punktom kontaktowym w innych państwach członkowskich, których dotyczy incydent[23].

Państwa członkowskie muszą powiadomić Komisję o wyznaczeniu pojedynczego punktu kontaktowego oraz o zadaniach powierzonych temu punktowi przed upływem terminu transpozycji. Decyzje o wyznaczeniu pojedynczego punktu kontaktowego należy podać do wiadomości publicznej, podobnie jak decyzje o wyznaczeniu właściwych organów krajowych. Komisja publikuje wykaz wyznaczonych pojedynczych punktów kontaktowych.

### 3.7. Sankcje

Zgodnie z art. 21 państwa członkowskie dysponują pewną swobodą uznania przy podejmowaniu decyzji dotyczących rodzaju i charakteru mających zastosowanie sankcji, o ile sankcje te będą skuteczne, proporcjonalne i odstraszające. Innymi słowy, państwa członkowskie mogą zasadniczo samodzielnie określać maksymalną kwotę sankcji przewidzianych w swoich przepisach krajowych, przy czym wybrana kwota lub wartość procentowa powinna zapewniać organom krajowym możliwość nałożenia – w każdym indywidualnym przypadku – skutecznych, proporcjonalnych i odstraszających sankcji, biorąc pod uwagę różne czynniki, takie jak powaga lub częstotliwość naruszenia.

## 4. Podmioty, na których spoczywają zobowiązania dotyczące wymogów w zakresie bezpieczeństwa i zgłaszania incydentów

Podmioty pełniące ważną funkcję społeczną i gospodarczą jako operatorzy usług kluczowych i dostawcy usług cyfrowych, o których mowa w art. 4 pkt 4 i 5 dyrektywy, są zobowiązane do wprowadzania odpowiednich środków bezpieczeństwa i zgłaszania poważnych incydentów właściwym organom krajowym. Wynika to z faktu, że skutki wystąpienia incydentów bezpieczeństwa w odniesieniu do tego rodzaju usług mogą stanowić poważne zagrożenie dla ich świadczenia, co z kolei może doprowadzić do poważnego zakłócenia prowadzonej działalności gospodarczej i funkcjonowania ogólnie rozumianego społeczeństwa, potencjalnie zmniejszając poziom zaufania użytkowników i wyrządzając poważne szkody gospodarce Unii[24].

Niniejszy punkt zawiera przegląd podmiotów objętych zakresem stosowania załączników II i III do dyrektywy w sprawie bezpieczeństwa sieci i informacji i wykaz spoczywających na nich obowiązków. Omówiono w nim szczegółowo proces identyfikacji operatorów usług kluczowych, biorąc pod uwagę znaczenie tego procesu dla zharmonizowanego wdrażania dyrektywy w sprawie bezpieczeństwa sieci i informacji w całej UE. W punkcie tym zawarto również wyczerpujące objaśnienia definicji infrastruktur cyfrowych i dostawców usług cyfrowych. Zbadano w niej również możliwość włączenia dodatkowych sektorów oraz przedstawiono dalsze informacje na temat konkretnego podejścia stosowanego w odniesieniu do dostawców usług cyfrowych.

[23] Zob. art. 14 ust. 5.
[24] Zob. motyw 2.

## 4.1. Operatorzy usług kluczowych

W dyrektywie w sprawie bezpieczeństwa sieci i informacji nie wskazano jednoznacznie konkretnych podmiotów, które można uznać za operatorów usług kluczowych objętych zakresem stosowania dyrektywy. Zamiast tego przedstawiono kryteria, które państwa członkowskie będą musiały zastosować, aby przeprowadzić proces identyfikacji, który w ostatecznym rozrachunku pozwoli ustalić, które przedsiębiorstwa należące do kategorii podmiotów wymienionych w załączniku II będą uznane za operatorów usług kluczowych, a zatem za podmioty podlegające obowiązkom przewidzianym w dyrektywie.

### 4.1.1. Rodzaje podmiotów wymienione w załączniku II do dyrektywy w sprawie bezpieczeństwa sieci i informacji

Zgodnie z definicją przedstawioną w art. 4 pkt 4 operator usług kluczowych to podmiot publiczny lub prywatny należący do jednego z rodzajów, o których mowa w załączniku II do dyrektywy, spełniający kryteria określone w art. 5 ust. 2. W załączniku II wymieniono sektory, podsektory i rodzaje podmiotów, w odniesieniu do których każde państwo członkowskie musi przeprowadzić proces identyfikacji zgodnie z art. 5 ust. 2[25]. Do sektorów tych zalicza się sektor energetyki, transportu, bankowości, infrastruktury rynków finansowych, służby zdrowia, zaopatrzenia w wodę pitną i jej dystrybucji oraz infrastruktury cyfrowej.

W przypadku większości podmiotów należących do „tradycyjnych sektorów" prawodawstwo UE zawiera kompleksowe definicje, do których odwołano się w załączniku II. Nie dotyczy to jednak sektora infrastruktury cyfrowej, o którym mowa w pkt 7 załącznika II, uwzględniając punkty wymiany ruchu internetowego, systemy nazw domen i rejestry nazw domen najwyższego poziomu. Dlatego też w celu doprecyzowania tych definicji poniżej przedstawiono ich szczegółowy opis.

#### 1) Punkt wymiany ruchu internetowego (IXP)

Termin „punkt wymiany ruchu internetowego" został zdefiniowany w art. 4 pkt 13 i doprecyzowany w motywie 18 – oznacza on obiekt sieciowy, który umożliwia połączenie międzysystemowe pomiędzy więcej niż dwoma niezależnymi systemami autonomicznymi, głównie do celów ułatwiania wymiany ruchu internetowego. Punkt wymiany ruchu internetowego można również opisać jako lokalizację fizyczną, w której szereg sieci może wymieniać się ze sobą ruchem internetowym za pomocą przełącznika. Głównym celem IXP jest zapewnienie sieciom możliwości bezpośredniego międzysystemowego łączenia się ze sobą za pośrednictwem punktu wymiany, bez konieczności korzystania z jednej sieci zarządzanej przez osobę trzecią lub większej liczby takich sieci. Dostawca IXP z reguły nie zajmuje się przekierowywaniem ruchu internetowego. Odpowiedzialność za podejmowanie działań związanych z przekierowywaniem ruchu internetowego spoczywa na dostawcach

[25] Aby uzyskać dodatkowe informacje na temat procesu identyfikacji, zob. pkt 4.1.6 poniżej.

usług sieciowych. Tworzenie bezpośrednich połączeń międzysystemowych wiąże się z licznymi korzyściami, wśród których najważniejsze to oszczędność kosztów, skrócenie czasu oczekiwania i poprawa przepustowości. Żadna ze stron nie pobiera zazwyczaj opłat z tytułu ruchu internetowego przechodzącego przez punkt wymiany, w odróżnieniu od ruchu internetowego przychodzącego do dostawcy usług internetowych wyższego szczebla. Ustanowienie bezpośredniego połączenia – niejednokrotnie w tym samym mieście, w którym znajdują się obydwie sieci – pozwala uniknąć konieczności przesyłania danych na dalekie odległości, co z kolei skraca czas oczekiwania.

Należy podkreślić, że definicja IXP nie obejmuje miejsc fizycznych, w których znajduje się połączenie międzysystemowe między dwiema sieciami fizycznymi (tj. definicja ta nie ma zastosowania do dostawców usług sieciowych takich jak BASE i PROXIMUS). Dlatego też przy transpozycji dyrektywy państwa członkowskie muszą dokonać rozróżnienia między operatorami, którzy ułatwiają przepływ skumulowanego ruchu internetowego między wieloma operatorami, a operatorami funkcjonującymi jako operatorzy jednej sieci, którzy tworzą połączenia międzysystemowe między swoimi sieciami na podstawie umowy dotyczącej połączeń międzysystemowych. W tym ostatnim przypadku dostawcy usług sieciowych nie są objęci definicją zawartą w art. 4 pkt 13. Dodatkowe wyjaśnienia w tej kwestii przedstawiono w motywie 18, który stanowi, że IXP nie zapewnia dostępu do sieci ani nie działa jako realizator tranzytu czy operator infrastruktury tranzytu. Ostatnią kategorią dostawców usług są przedsiębiorstwa udostępniające publiczne sieci łączności lub usługi, które podlegają wymogom dotyczącym bezpieczeństwa i zgłaszania incydentów ustanowionym w art. 13a i 13b dyrektywy 2002/21/WE i które są tym samym wyłączone z zakresu stosowania dyrektywy w sprawie bezpieczeństwa sieci i informacji[26].

**2) System nazw domen (DNS)**

Termin „system nazw domen" został zdefiniowany w art. 4 pkt 14 jako „hierarchiczny rozproszony system nazw sieciowych, który odpowiada na zapytania o nazwy domen". Ściślej rzecz biorąc, DNS można opisać jako hierarchiczny rozproszony system nazw domen dla komputerów, usług lub jakichkolwiek innych zasobów podłączonych do internetu umożliwiający kodowanie nazw domen w adresach IP (protokół internetowy). Główną rolą systemu jest przekształcanie przypisanych nazw domen w adresy IP. W tym celu DNS obsługuje bazę danych i wykorzystuje nazwy serwerów i program rozpoznawania nazw, aby zapewnić możliwość „przetłumaczenia" nazw domen na funkcjonalne adresy IP. Choć kodowanie nazw domen nie jest jedyną funkcją DNS, jest to główne zadanie systemu. W definicji prawnej przedstawionej w art. 4 pkt 14 skoncentrowano się na głównej funkcji systemu z punktu widzenia użytkownika, nie poruszając bardziej szczegółowych kwestii technicznych, takich jak na przykład zarządzanie przestrzenią nazw domen, nazwami serwerów, programami rozpoznawania nazw itp. Z kolei w art. 4 pkt 15 wyjaśniono, kogo uznaje się za dostawcę usług DNS.

[26] Aby uzyskać dodatkowe informacje na temat związku pomiędzy dyrektywą w sprawie bezpieczeństwa sieci i informacji a dyrektywą 2002/21/WE, zob. pkt 5.2.

**3) Rejestr nazw domen najwyższego poziomu** (rejestr nazw TLD)

Zgodnie z definicją przedstawioną w art. 4 pkt 16 rejestr nazw domen najwyższego poziomu oznacza podmiot, który zarządza rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu i dokonuje takiej rejestracji. Takie zarządzanie nazwami domen obejmuje kodowanie nazw TLD w adresach IP.

IANA (agencja ds. przydzielonych numerów internetowych) jest odpowiedzialna za koordynowanie działań związanych z serwerem głównym DNS, adresacją protokołu internetowego i innymi zasobami związanymi z protokołem internetowym na szczeblu globalnym. W szczególności IANA odpowiada za przydzielanie operatorom rodzajowych domen najwyższego poziomu (gTLD), np. „.com", oraz krajowych domen najwyższego poziomu (ccTLD), np. „be", oraz za utrzymywanie szczegółowych informacji technicznych i administracyjnych dotyczących tych domen. IANA prowadzi globalny rejestr przydzielonych TLD i bierze udział w procesie ujawniania treści tego wykazu użytkownikom internetu na całym świecie, a także w procesie wprowadzania nowych TLD.

Ważnym zadaniem rejestrów jest przydzielanie nazw drugiego poziomu tzw. rejestrującym w ramach ich odpowiednich TLD. Wspomniani rejestrujący mogą również – wedle swojego uznania – samodzielnie przydzielać nazwy domen trzeciego poziomu. Krajowe domeny najwyższego poziomu odnoszą się do nazwy państwa lub terytorium ustalonej zgodnie z normą ISO 3166-1. „Rodzajowe" TLD zazwyczaj nie są przyporządkowane do określonego obszaru geograficznego ani do określonego państwa.

Należy podkreślić, że prowadzenie rejestru nazw TLD może obejmować również obsługę DNS. Na przykład zgodnie z zasadami delegowania opracowanymi przez IANA wyznaczony podmiot odpowiedzialny za ccTLD musi m.in. sprawować nadzór nad nazwami domen i obsługiwać DNS danego państwa[27]. Państwa członkowskie muszą wziąć te okoliczności pod uwagę przy przeprowadzaniu procesu identyfikacji operatorów usług kluczowych zgodnie z art. 5 ust. 2.

### 4.1.2. Identyfikacja operatorów usług kluczowych

Zgodnie z wymogami art. 5 dyrektywy każde państwo członkowskie jest zobowiązane do przeprowadzenia procesu identyfikacji w odniesieniu do wszystkich podmiotów należących do rodzajów wymienionych w załączniku II, które posiadają zarejestrowaną jednostkę organizacyjną na terytorium danego państwa członkowskiego. Po przeprowadzeniu tej oceny wszystkie podmioty spełniające kryteria ustanowione w art. 5 ust. 2 uznaje się za operatorów usług kluczowych podlegających obowiązkom w zakresie bezpieczeństwa i zgłaszania incydentów przewidzianym w art. 14.

Państwa członkowskie są zobowiązane zidentyfikować operatorów we wszystkich sektorach i podsektorach do dnia 9 listopada 2018 r. Aby udzielić państwom członkowskim wsparcia przy przeprowadzaniu tej procedury, grupa współpracy opracowuje obecnie wytyczne

[27] Informacje dostępne pod adresem: https://www.icann.org/resources/pages/delegation-2012-02-25-en

zawierające stosowne informacje na temat koniecznych działań i najlepszych praktyk w zakresie identyfikowania operatorów usług kluczowych.

Ponadto zgodnie z art. 24 ust. 2 grupa współpracy jest zobowiązana do omawiania tego procesu, treści i rodzaju środków krajowych umożliwiających identyfikację operatorów usług kluczowych w danych sektorach. Do dnia 9 listopada 2018 r. państwo członkowskie może dążyć do organizowania na forum grupy współpracy dyskusji poświęconych przygotowywanym przez siebie projektom środków krajowych umożliwiających identyfikowanie operatorów usług kluczowych.

### 4.1.3. Włączanie dodatkowych sektorów

Biorąc pod uwagę wymóg harmonizacji minimalnej ustanowiony w art. 3, państwa członkowskie mogą przyjąć lub utrzymać w mocy przepisy zapewniające wyższy poziom bezpieczeństwa sieci i systemów informatycznych. W tym względzie państwa członkowskie co do zasady dysponują swobodą w kwestii rozszerzania zakresu przewidzianych w art. 14 obowiązków dotyczących bezpieczeństwa i zgłaszania incydentów na podmioty należące do sektorów i podsektorów innych niż te wymienione w załączniku II do dyrektywy w sprawie bezpieczeństwa sieci i informacji. Szereg państw członkowskich zdecydowało się włączyć niektóre z wymienionych poniżej dodatkowych sektorów do zakresu obowiązywania dyrektywy lub rozważa możliwość objęcia tych sektorów przepisami dyrektywy:

*(i) Administracje publiczne*

Administracje publiczne mogą oferować usługi kluczowe wymienione w załączniku II do dyrektywy, jeżeli spełniają wymogi ustanowione w art. 5 ust. 2. W takich przypadkach administracje publiczne oferujące tego rodzaju usługi podlegałyby odpowiednim wymogom w zakresie bezpieczeństwa i obowiązkom w zakresie zgłaszania incydentów. Z kolei w przypadku, gdy administracje publiczne oferują usługi, które nie mieszczą się w powyższym zakresie, takie usługi nie mogą podlegać stosownym obowiązkom.

Administracje publiczne są odpowiedzialne za prawidłowe świadczenie usług publicznych przez organy rządowe, organy na szczeblu regionalnym i lokalnym, agencje i powiązane przedsiębiorstwa. Świadczenie tych usług często wiąże się z koniecznością tworzenia danych osobowych i korporacyjnych o osobach fizycznych i organizacjach i zarządzania takimi danymi, które można następnie udostępniać różnym podmiotom publicznym. Szerzej rzecz ujmując, zapewnienie wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez administracje publiczne leży w interesie społeczeństwa i ogólnie rozumianej gospodarki. Dlatego też Komisja uważa, że państwa członkowskie powinny rozważyć możliwość włączenia administracji publicznej do przepisów krajowych transponujących dyrektywę, których zakres wykraczałby poza świadczenie usług kluczowych zgodnie z przepisami załącznika II i art. 5 ust. 2.

*(ii) Sektor pocztowy*

W sektorze pocztowym świadczy się usługi pocztowe takie jak odbieranie, sortowanie, przewożenie i dystrybuowanie przesyłek pocztowych.

*(iii) Sektor spożywczy*

Sektor spożywczy odpowiada za produkcję produktów rolnych i innych produktów spożywczych i może świadczyć usługi kluczowe takie jak zapewnianie bezpieczeństwa żywnościowego i dbanie o jakość i bezpieczeństwo żywności.

*(iv) Przemysł chemiczny i jądrowy*

Przemysł chemiczny i jądrowy zajmuje się w szczególności składowaniem, produkcją i przetwarzaniem produktów chemicznych i petrochemicznych lub materiałów jądrowych.

*(v) Sektor ochrony środowiska*

Działania w obszarze ochrony środowiska obejmują dostarczanie towarów i świadczenie usług niezbędnych w kontekście ochrony środowiska i zarządzania zasobami. Działania podejmowane w tym sektorze służą przeciwdziałaniu zanieczyszczeniom, ograniczaniu ich skutków i ich zwalczaniu oraz zachowaniu istniejących zasobów naturalnych. Wśród usług kluczowych świadczonych w tym sektorze można wymienić monitorowanie i kontrolowanie poziomu zanieczyszczeń (np. zanieczyszczeń powietrza i wody) oraz zjawisk pogody.

*(vi) Ochrona ludności*

Celem działań podejmowanych w sektorze ochrony ludności jest zapobieganie klęskom żywiołowym i katastrofom spowodowanym przez człowieka, przygotowywanie się do nich i reagowanie na nie. Wśród usług świadczonych w tym celu można wymienić aktywowanie numerów alarmowych i podejmowanie działań informujących o sytuacjach wyjątkowych, służących ograniczaniu skali takich sytuacji oraz reagowaniu na nie.

### 4.1.4. Jurysdykcja

Zgodnie z art. 5 ust. 1 każde państwo członkowskie musi zidentyfikować operatorów usług kluczowych posiadających jednostkę organizacyjną na jego terytorium. Choć w przepisie tym nie doprecyzowano rodzaju zarejestrowanej jednostki organizacyjnej, w motywie 21 wyjaśniono, że posiadanie takiej jednostki organizacyjnej wiąże się z koniecznością prowadzenia działalności w sposób efektywny i rzeczywisty poprzez stabilne struktury, natomiast forma prawna takich struktur nie powinna być czynnikiem decydującym. Oznacza to, że operator usług kluczowych może podlegać jurysdykcji danego państwa członkowskiego nie tylko w przypadku, gdy posiada swoją siedzibę zarządu na terytorium tego państwa, ale również w przypadkach, gdy w danym państwie znajduje się jego oddział lub innego rodzaju prawna jednostka organizacyjna.

Konsekwencją tego stanu rzeczy jest fakt, że ten sam podmiot może jednocześnie podlegać jurysdykcji kilku państw członkowskich.

### 4.1.5. Informacje, które należy przedłożyć Komisji

Na potrzeby przeglądu, który Komisja jest zobowiązana przeprowadzić zgodnie z art. 23 ust. 1 dyrektywy w sprawie bezpieczeństwa sieci i informacji, państwa członkowskie są zobowiązane przedłożyć Komisji w terminie do dnia 9 listopada 2018 r., a następnie co dwa lata, następujące informacje:

- informacje o krajowych środkach umożliwiających identyfikowanie operatorów usług kluczowych;
- wykaz usług kluczowych;

- informacje o liczbie zidentyfikowanych operatorów usług kluczowych w każdym z sektorów, o których mowa w załączniku II, oraz wskazanie ich znaczenia w odniesieniu do tego sektora; oraz

- informacje o progach, 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 podmiotu zgodnie z art. 6 ust. 1 lit. f).

Przegląd, o którym mowa w art. 23 ust. 1 i który poprzedza kompleksowy przegląd dyrektywy, odzwierciedla znaczenie, jakie współprawodawcy przywiązują do prawidłowej transpozycji dyrektywy w kwestiach związanych z identyfikowaniem operatorów usług kluczowych, aby uniknąć fragmentacji rynku.

W celu możliwie jak najsprawniejszego przeprowadzenia tej procedury Komisja zachęca państwa członkowskie do omawiania tej kwestii oraz do wymieniania się odpowiednimi doświadczeniami na forum grupy współpracy. Ponadto Komisja zachęca państwa członkowskie do udostępniania Komisji, poza wszystkimi informacjami, które państwa członkowskie są zobowiązane przedłożyć Komisji zgodnie z przepisami dyrektywy, wykazów zidentyfikowanych operatorów usług kluczowych (którzy zostali ostatecznie wybrani), w razie potrzeby na zasadzie poufności. Udostępnienie takich wykazów usprawniłoby ocenę przez Komisję spójności procesu identyfikacji i zapewniłoby lepszą jakość tego procesu, a także umożliwiłoby porównanie podejść stosowanych przez poszczególne państwa członkowskie, przyczyniając się tym samym do lepszej realizacji celów dyrektywy.

### 4.1.6. Jak przeprowadzić proces identyfikacji?

Jak wskazano na wykresie 4, organy krajowe powinny odpowiedzieć na sześć kluczowych pytań przy przeprowadzaniu procesu identyfikacji w odniesieniu do danego podmiotu. Każde z pytań przedstawionych w poniższych akapitach odpowiada krokowi, który należy podjąć zgodnie z art. 5 w związku z art. 6, biorąc również pod uwagę możliwość zastosowania przepisów art. 1 ust. 7.

Krok 1 – **Czy dany podmiot należy do sektora/podsektora i czy jego rodzaj odpowiada jednemu z rodzajów wymienionych w załączniku II do dyrektywy?**

Organ krajowy powinien ocenić, czy podmiot posiadający jednostkę organizacyjną na jego terytorium należy do sektorów i podsektorów wymienionych w załączniku II do dyrektywy. W załączniku II wymieniono różne sektory gospodarki, które uznaje się za niezbędne dla zapewnienia prawidłowego funkcjonowania rynku wewnętrznego. W załączniku II odniesiono się w szczególności do następujących sektorów i podsektorów:

- energetyka: energia elektryczna, ropa naftowa i gaz;
- transport: transport lotniczy, transport kolejowy, transport wodny i transport drogowy;
- bankowość: instytucje kredytowe;
- infrastruktura rynków finansowych: systemy obrotu, kontrahenci centralni;
- służba zdrowia: świadczeniodawcy (w tym szpitale i prywatne kliniki);
- woda: zaopatrzenie w wodę pitną i jej dystrybucja;

- infrastruktura cyfrowa: punkty wymiany ruchu internetowego, dostawcy usług DNS, rejestry nazw domen najwyższego poziomu[28].

Krok 2 – **Czy w danym przypadku zastosowanie mają przepisy szczególne?**

Kolejnym krokiem, jaki powinien podjąć organ krajowy, jest ocena, czy w danym przypadku zastosowanie mają przepisy szczególne przewidziane w art. 1 ust. 7. Ustęp ten stanowi w szczególności, że w przypadku istnienia aktu prawnego UE nakładającego na dostawców usług cyfrowych lub operatorów usług kluczowych wymogi w zakresie bezpieczeństwa lub zgłaszania incydentów, które są co najmniej równoważne odpowiednim wymogom przewidzianym w dyrektywie w sprawie bezpieczeństwa sieci i informacji, zastosowanie powinny mieć obowiązki przewidziane w tym szczególnym akcie prawnym. Ponadto w motywie 9 wyjaśniono, że w przypadku spełnienia wymogów przewidzianych w art. 1 ust. 7 państwa członkowskie powinny stosować przepisy sektorowego aktu prawnego Unii, w tym przepisy odnoszące się do jurysdykcji. Z kolei odpowiednie przepisy dyrektywy w sprawie bezpieczeństwa sieci i informacji nie miałyby zastosowania. W takim przypadku właściwy organ nie powinien kontynuować procesu identyfikacji zgodnie z art. 5 ust. 2[29].

Krok 3 – **Czy operator świadczy usługę kluczową w rozumieniu dyrektywy?**

Zgodnie z art. 5 ust. 2 lit. a) podmiot będący przedmiotem procedury identyfikowania musi świadczyć usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej. Przeprowadzając taką ocenę, państwa członkowskie powinny wziąć pod uwagę fakt, że ten sam podmiot może świadczyć zarówno usługi kluczowe, jak i usługi inne niż kluczowe. Oznacza to, że wymogi w zakresie bezpieczeństwa i zgłaszania incydentów przewidziane w dyrektywie w sprawie bezpieczeństwa sieci i informacji będą miały zastosowanie do danego operatora wyłącznie w zakresie, w jakim świadczy on usługi kluczowe.

Zgodnie z art. 5 ust. 3 państwo członkowskie powinno sporządzić wykaz wszystkich usług kluczowych świadczonych przez operatorów usług kluczowych na jego terytorium. Wykaz ten należy przedłożyć Komisji w terminie do dnia 9 listopada 2018 r., a następnie co dwa lata[30].

Krok 4 – **Czy świadczenie usługi zależy od sieci i systemu informatycznego?**

Ponadto należy wyjaśnić, czy dana usługa spełnia drugie kryterium przewidziane w art. 5 ust. 2 lit. b), a w szczególności czy świadczenie usługi kluczowej zależy od sieci i systemów informatycznych zdefiniowanych w art. 4 ust. 1.

---

[28] W pkt 4.1.1 przedstawiono dodatkowe wyjaśnienia dotyczące tych podmiotów.

[29] Bardziej szczegółowe informacje na temat możliwości zastosowania przepisów szczególnych, przedstawiono w pkt 5.1.

[30] Zob. art. 5 ust. 7 lit. b).

Krok 5 – **Czy incydent bezpieczeństwa miałby istotny skutek zakłócający?**

Zgodnie z art. 5 ust. 2 lit. c) organ krajowy jest zobowiązany ocenić, czy incydent miałby istotny skutek zakłócający dla świadczenia danej usługi. W tym kontekście w art. 6 ust. 1 wskazano szereg czynników międzysektorowych, które należy wziąć pod uwagę przy przeprowadzaniu oceny. Ponadto art. 6 ust. 2 stanowi, że – w stosownych przypadkach – w ocenie powinno się uwzględnić także czynniki sektorowe.

Do **czynników międzysektorowych** wymienionych w art. 6 ust. 1 zalicza się następujące czynniki:

- liczbę użytkowników zależnych od usługi świadczonej przez dany podmiot;
- zależność innych sektorów, o których mowa w załączniku II, od usługi świadczonej przez ten podmiot;
- wpływ, jaki incydenty – jeżeli chodzi o ich skalę i czas trwania – mogłyby mieć na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne;
- udział danego podmiotu w rynku;
- zasięg geograficzny związany z obszarem, którego mógłby dotyczyć incydent;
- znaczenie podmiotu w utrzymywaniu wystarczającego poziomu usługi przy uwzględnieniu dostępności alternatywnych sposobów świadczenia tej usługi.

Jeżeli chodzi o **czynniki sektorowe**, w motywie 28 przedstawiono pewne przykłady (zob. tabela 4), które mogą posłużyć jako użyteczne wskazówki dla organów krajowych.

**Tabela 4: Przykłady czynników sektorowych, które należy wziąć pod uwagę przy ustalaniu, czy dany incydent ma istotny skutek zakłócający.**

| Sektor | Przykłady czynników sektorowych |
|---|---|
| **Dostawcy energii** | wielkość lub udział w krajowej produkcji energii |
| **Dostawcy ropy naftowej** | dzienna wielkość dostaw ropy naftowej |
| **Transport lotniczy (w tym porty lotnicze i przewoźnicy lotniczy)**<br>**Transport kolejowy**<br>**Porty morskie** | udział w wolumenie ruchu krajowego;<br>roczna liczba pasażerów lub przewozów towarowych. |
| **Bankowość lub infrastruktura rynków finansowych** | znaczenie systemowe na podstawie sumy aktywów;<br>stosunek sumy aktywów do PKB |
| **Sektor ochrony zdrowia** | roczna liczba pacjentów objętych opieką usługodawcy |
| **Produkcja, uzdatnianie i dostawy wody** | jej ilość, a także liczba i rodzaje zaopatrywanych użytkowników (w tym na przykład szpitale, służba publiczna, organizacje lub osoby indywidualne);<br>istnienie alternatywnych źródeł wody na tym samym obszarze geograficznym |

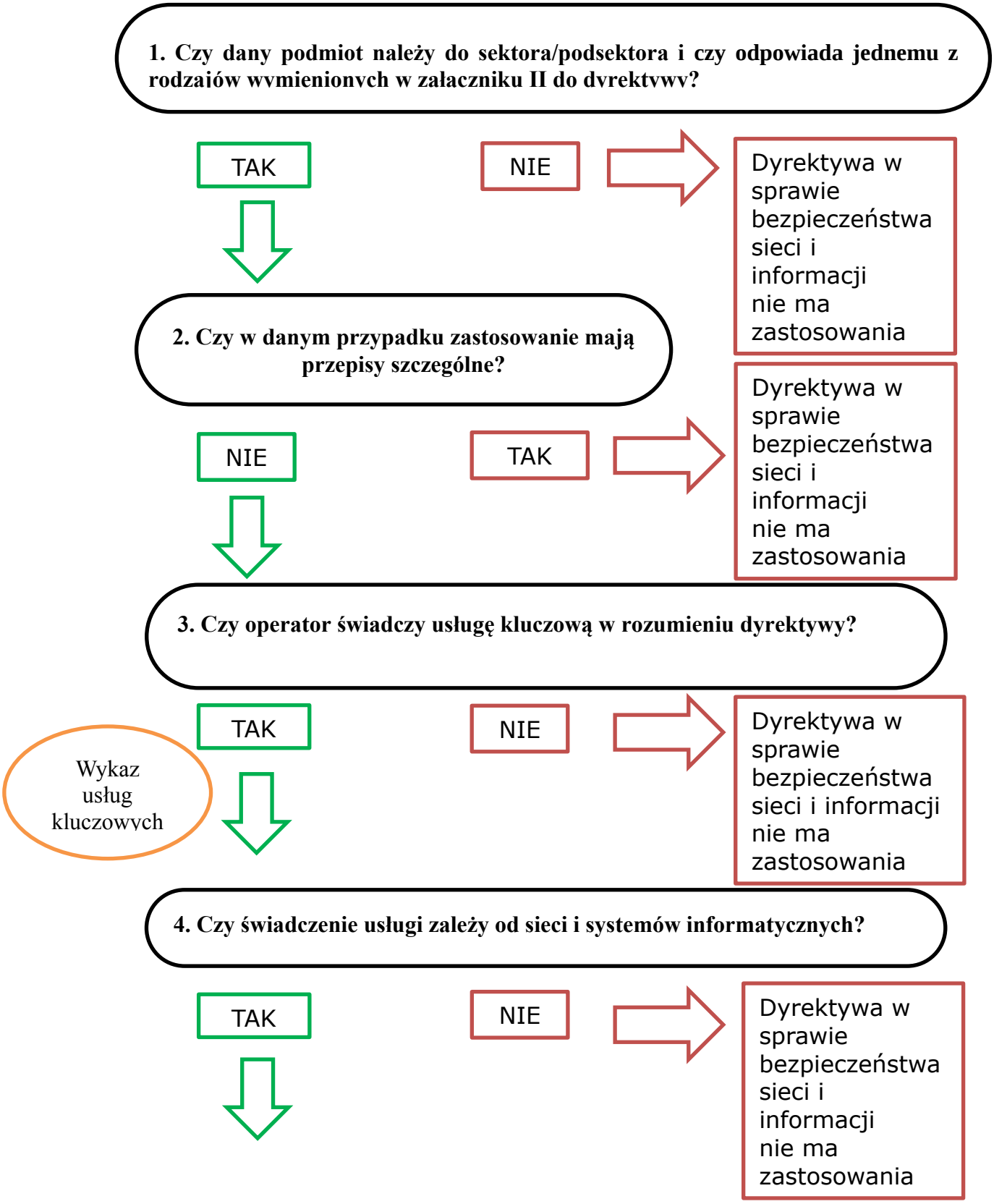
Należy podkreślić, że przy przeprowadzaniu oceny zgodnie z art. 5 ust. 2 państwa członkowskie nie powinny stosować dodatkowych kryteriów poza kryteriami wymienionymi w tym przepisie, ponieważ mogłoby to zawęzić liczbę identyfikowanych operatorów usług kluczowych i zagrozić harmonizacji minimalnej operatorów usług kluczowych, o której mowa w art. 3 dyrektywy.

Krok 6 – **Czy dany operator świadczy usługi kluczowe w innych państwach członkowskich?**

Krok 6 dotyczy przypadków, w których operator świadczy swoje usługi kluczowe w dwóch państwach członkowskich lub w większej ich liczbie. Zgodnie z art. 5 ust. 4 przed zakończeniem procesu identyfikacji odpowiednie państwa członkowskie są zobowiązane wziąć udział w procesie konsultacji[31].

[31] Aby uzyskać bardziej szczegółowe informacje na temat procesu konsultacji, zob. pkt 4.1.7.

**Wykres 4: Proces identyfikacji w 6 krokach**



**5. Czy incydent bezpieczeństwa miałby istotny skutek zakłócający?**

**Czynniki międzysektorowe (art. 6 ust. 1)**

- **Liczba użytkowników** zależnych od usług
- **Zależność** innych kluczowych sektorów od usługi
- Wpływ, jaki incydenty mogłyby mieć na **działalność gospodarczą i społeczną** lub **bezpieczeństwo publiczne**
- Potencjalny **zasięg geograficzny**
- Znaczenie podmiotu w utrzymywaniu wystarczającego **poziomu usługi**

**Czynniki sektorowe (przykłady wymienione w motywie 28)**

- **Energetyka**: wielkość lub udział w krajowej produkcji energii
- **Transport**: udział w wolumenie ruchu krajowego i liczba przewozów w skali roku
- **Służba zdrowia**: roczna liczba pacjentów objętych opieką usługodawcy

TAK

NIE → Dyrektywa w sprawie bezpieczeństwa sieci i informacji nie ma zastosowania

**6. Czy dany operator świadczy usługi kluczowe w innych państwach członkowskich?**

TAK

NIE → Dyrektywa w sprawie bezpieczeństwa sieci i informacji nie ma zastosowania

Obowiązkowe konsultacje z zainteresowanymi państwami członkowskimi

Przyjęcie środków krajowych (np. wykaz operatorów usług kluczowych, środki polityczne i prawne).

### 4.1.7. Proces konsultacji transgranicznych

Jeżeli operator świadczy usługi kluczowe w dwóch państwach członkowskich lub w większej ich liczbie, zgodnie z art. 5 ust. 4 stosowne państwa członkowskie wzajemnie się konsultują przed zakończeniem procesu identyfikacji. Celem tych konsultacji jest ułatwienie oceny krytycznego charakteru danego operatora, jeżeli chodzi o wpływ transgraniczny.

Oczekuje się, że dzięki zorganizowaniu konsultacji zaangażowane organy krajowe będą wymieniały się argumentami i stanowiskami i – w optymalnym przypadku – dojdą do tych samych wniosków w kwestii identyfikacji danego operatora. Dyrektywa w sprawie bezpieczeństwa sieci i informacji nie uniemożliwia jednak państwom członkowskim dojścia do rozbieżnych wniosków w kwestii tego, czy dany podmiot można zidentyfikować jako operatora usług kluczowych, czy też nie. W motywie 24 wspomniano o możliwości zwrócenia się przez państwa członkowskie o pomoc w tym zakresie do grupy współpracy.

Zdaniem Komisji państwa członkowskie powinny dążyć do wypracowania porozumienia w tych kwestiach, aby nie dopuścić do sytuacji, w której to samo przedsiębiorstwo posiada różny status sprawny w poszczególnych państwach członkowskich. Do przyjęcia rozbieżnych ustaleń powinno dochodzić wyłącznie w wyjątkowych okolicznościach, np. gdy podmiot uznany za operatora usług kluczowych w jednym państwie członkowskim prowadzi bardzo ograniczoną i mało istotną działalność w innym państwie członkowskim.

## 4.2. Wymogi w zakresie bezpieczeństwa

Zgodnie z art. 14 ust. 1 państwa członkowskie są zobowiązane do zapewnienia, aby operatorzy usług kluczowych – uwzględniając najnowszy stan wiedzy – wprowadzali odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykami, na jakie narażone jest bezpieczeństwo sieci i systemów informatycznych wykorzystywanych przez nich do świadczenia swoich usług. Zgodnie z art. 14 ust. 2 odpowiednie środki muszą zapobiegać incydentom i minimalizować ich wpływ.

Osobnym obszarem prac prowadzonych obecnie przez grupę współpracy są niewiążące wytyczne dotyczące środków bezpieczeństwa dla operatorów usług kluczowych[32]. Grupa ma zakończyć prace nad wytycznymi do czwartego kwartału 2017 r. Komisja zachęca państwa członkowskie do ścisłego stosowania się do treści wytycznych, które zostaną opracowane przez grupę współpracy, aby zapewnić możliwie jak najlepsze dostosowanie przepisów krajowych do wymogów w zakresie bezpieczeństwa. Harmonizacja takich wymogów w istotnym stopniu ułatwiłaby przestrzeganie wymogów przez operatorów usług kluczowych, którzy często świadczą usługi kluczowe w więcej niż jednym państwie członkowskim, a także nadzorowanie działań właściwych organów krajowych i CSIRT.

[32] Na potrzeby tego obszaru prac rozpowszechniano wykazy norm międzynarodowych, dobrych praktyk oraz metod oceny ryzyka / zarządzania ryzykiem dotyczących wszystkich sektorów objętych zakresem dyrektywy w sprawie bezpieczeństwa sieci i informacji i wykorzystano je jako materiał źródłowy przy przygotowywaniu propozycji dotyczących obszarów bezpieczeństwa i środków bezpieczeństwa.

### 4.3. Wymogi dotyczące zgłaszania incydentów

Zgodnie z art. 14 ust. 3 państwa członkowskie muszą zapewnić, aby operatorzy usług kluczowych zgłaszali wszelkie „incydenty mające istotny wpływ na ciągłość świadczonych przez nich usług kluczowych". Z tego względu operatorzy usług kluczowych nie powinni zgłaszać mało znaczących incydentów, ale wyłącznie poważne incydenty mające wpływ na ciągłość świadczenia danej usług kluczowej. Zgodnie z definicją przedstawioną w art. 4 pkt 7 termin „incydent" oznacza „każde zdarzenie, które ma rzeczywiście niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych". Termin „bezpieczeństwo sieci i systemów informatycznych" został zdefiniowany w art. 4 pkt 2 jako „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". Tym samym każde zdarzenie wywierające niekorzystny wpływ nie tylko na dostępność, ale również na autentyczność, integralność lub poufność danych lub powiązanych z nimi usług może potencjalnie prowadzić do powstania obowiązku zgłoszenia incydentu. W rzeczywistości do przerwania ciągłości świadczenia usługi, o której mowa w art. 14 ust. 3, może dojść nie tylko w przypadkach związanych z fizyczną dostępnością tej usługi, ale również w przypadku wystąpienia jakiegokolwiek innego incydentu bezpieczeństwa wywierającego wpływ na możliwość prawidłowego świadczenia usługi[33].

Osobnym obszarem prac prowadzonych obecnie przez grupę współpracy jest przygotowanie niewiążących wytycznych dotyczących okoliczności, w których operatorzy usług kluczowych są zobowiązani do zgłaszania incydentów zgodnie z art. 14 ust. 7, oraz formatu i procedury takich zgłoszeń krajowych. Wytyczne te mają zostać opracowane do czwartego kwartału 2017 r.

Rozbieżne krajowe wymogi dotyczące zgłaszania incydentów mogą prowadzić do niepewności prawa, bardziej skomplikowanych i uciążliwych procedur oraz znacznych kosztów administracyjnych dla dostawców transgranicznych. Dlatego też Komisja z zadowoleniem przyjmuje prace prowadzone na forum grupy współpracy. Podobnie jak w przypadku wymogów w zakresie bezpieczeństwa Komisja zachęca państwa członkowskie do ścisłego stosowania się do treści wytycznych, które zostaną opracowane przez grupę współpracy, aby zapewnić możliwie jak najlepsze dostosowanie przepisów krajowych dotyczących zgłaszania incydentów.

### 4.4. Załącznik III do dyrektywy w sprawie bezpieczeństwa sieci i informacji: dostawcy usług cyfrowych

Dostawcy usług cyfrowych stanowią drugą kategorię podmiotów objętych zakresem stosowania dyrektywy w sprawie bezpieczeństwa sieci i informacji. Podmioty te uznaje się za ważne z gospodarczego punktu widzenia z uwagi na fakt, że wiele przedsiębiorstw

[33] To samo dotyczy dostawców usług cyfrowych.

wykorzystuje je do świadczenia swoich własnych usług, dlatego też jakiekolwiek zakłócenie ciągłości świadczenia przez nie usług cyfrowych może wpłynąć na kluczową działalność gospodarczą i społeczną.

### 4.4.1. Kategorie dostawców usług cyfrowych.

W art. 4 pkt 5, w którym zdefiniowano „usługę cyfrową", odniesiono się do definicji prawnej zawartej w art. 1 ust. 1 lit. b) dyrektywy (UE) 2015/1535, zawężając zakres tej definicji do rodzajów usług wymienionych w załączniku III. W szczególności w art. 1 ust. 1 lit. b) dyrektywy (UE) 2015/1535 tego rodzaju usługi zdefiniowano jako „każdą usługę normalnie świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług", natomiast w załączniku III do dyrektywy wymieniono trzy konkretne rodzaje usług: internetową platformę handlową, wyszukiwarkę internetową i usługę przetwarzania w chmurze. W porównaniu z operatorami usług kluczowych w dyrektywie nie zobowiązano państw członkowskich do zidentyfikowania dostawców usług cyfrowych, którzy następnie podlegaliby stosownym wymogom. Dlatego też stosowne obowiązki przewidziane w dyrektywie, mianowicie wymogi w zakresie bezpieczeństwa i zgłaszania incydentów ustanowione w art. 16, będą miały zastosowanie do wszystkich dostawców usług cyfrowych objętych zakresem stosowania dyrektywy.

W poniższych punktach przedstawiono dodatkowe wyjaśnienia dotyczące trzech rodzajów usług cyfrowych objętych zakresem stosowania dyrektywy.

**1. Dostawca internetowej platformy handlowej**

Internetowa platforma handlowa zapewnia dużej liczbie zróżnicowanych przedsiębiorstw możliwość prowadzenia działalności handlowej wobec konsumentów i nawiązywania stosunków biznesowych. Platforma ta stanowi podstawową infrastrukturę umożliwiającą prowadzenie internetowej i transgranicznej wymiany handlowej. Odgrywa ona istotną rolę w gospodarce, w szczególności dzięki zapewnieniu MŚP dostępu do szerzej zakrojonego unijnego jednolitego rynku cyfrowego. Działania podejmowane przez dostawcę internetowej platformy handlowej mogą również obejmować świadczenie usług komputerowych na odległość ułatwiających klientowi prowadzenie działalności gospodarczej, w tym przetwarzanie transakcji i gromadzenie danych na temat nabywców, dostawców i produktów, jak również ułatwianie wyszukiwania odpowiednich produktów, oferowanie produktów, dzielenie się wiedzą fachową w dziedzinie realizowania transakcji oraz dobieranie kupujących i sprzedających.

Termin „internetowa platforma handlowa" został zdefiniowany w art. 4 pkt 17 i dodatkowo wyjaśniony w motywie 15. Zgodnie z tym motywem internetowa platforma handlowa jest usługą umożliwiającą konsumentom i przedsiębiorcom handlowym zawieranie umów sprzedaży lub umów o świadczenie usług *online* z przedsiębiorcami handlowymi i będącą ostatecznym miejscem zawierania tych umów. Na przykład dostawcę takiego jak E-bay można uznać za internetową platformę handlową, ponieważ zapewnia innym podmiotom możliwość tworzenia sklepów na platformie w celu udostępniania swoich produktów i usług *online* konsumentom lub przedsiębiorstwom. Internetowe sklepy z aplikacjami zajmujące się

dystrybucją aplikacji i oprogramowania również uznaje się za spełniające kryteria wymienione w definicji internetowej platformy handlowej, ponieważ zapewniają one twórcom aplikacji możliwość sprzedawania lub dystrybuowania swoich usług konsumentom lub innym przedsiębiorstwom. Natomiast usługi pełniące wyłącznie funkcję pośredniczącą wobec usług stron trzecich, takie jak usługa porównywania cen Skyscanner przekierowująca użytkownika na stronę internetową przedsiębiorcy, na której zawierana jest właściwa umowa dotycząca danej usługi lub produktu, nie są objęte zakresem definicji ustanowionej w art. 4 pkt 17.

**2. Dostawca wyszukiwarki internetowej**

Termin „wyszukiwarka internetowa" został zdefiniowany w art. 4 pkt 18 i wyjaśniony bardziej szczegółowo w motywie 16. 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. Definicja ta nie obejmuje funkcji wyszukiwania, które ograniczają się do treści na konkretnej stronie internetowej, ani stron internetowych służących do porównywania cen. Na przykład wyszukiwarki internetowej podobnej do wyszukiwarki udostępnianej na portalu EUR-Lex[34] nie można uznać za wyszukiwarkę internetową w rozumieniu dyrektywy, ponieważ jej funkcja wyszukiwania ogranicza się wyłącznie do treści konkretnej strony internetowej.

**3. Usługa przetwarzania w chmurze**

W art. 4 pkt 19 zdefiniowano „usługę przetwarzania w chmurze" jako „usługę cyfrową umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania", a w motywie 17 doprecyzowano terminy „zasoby obliczeniowe", „skalowalne" i „elastyczny zbiór".

Mówiąc w skrócie, przetwarzanie w chmurze można opisać jako określony rodzaj usługi komputerowej, w której wykorzystuje się udostępnione zasoby do przetwarzania danych na żądanie, przy czym udostępnione zasoby oznaczają wszelkiego rodzaju elementy sprzętu komputerowego lub oprogramowania (np. sieci, serwery lub inną infrastrukturę, pamięć, aplikacje i usługi), które udostępnia się użytkownikom na żądanie do celów związanych z przetwarzaniem danych. Termin „wspólne wykorzystywanie" definiuje zasoby obliczeniowe, w przypadku których wielu użytkowników korzysta z tej samej infrastruktury fizycznej do przetwarzania danych. „Zasoby obliczeniowe" można zdefiniować jako zasoby do wspólnego wykorzystywania, jeżeli zbiór zasobów wykorzystywanych przez dostawcę można rozszerzyć lub zmniejszyć w dowolnym momencie, w zależności od wymagań użytkownika. Zapewnia to możliwość dodawania lub usuwania ośrodków przetwarzania danych lub pojedynczych elementów w ramach jednego ośrodka przetwarzania danych w przypadku konieczności zaktualizowania całkowitej ilości zasobów obliczeniowych lub pamięci. Termin „elastyczny zbiór" można opisać jako zmiany obciążenia poprzez automatyczne dodawanie i usuwanie zasobów, tak aby w każdym momencie poziom

[34] Dostępnej pod adresem: http://eur-lex.europa.eu/homepage.html?locale=pl

udostępnianych zasobów był możliwie jak najdokładniej dopasowany do bieżącego zapotrzebowania[35].

Obecnie można wyróżnić trzy głównie rodzaje modeli usług w chmurze, które może świadczyć dostawca:

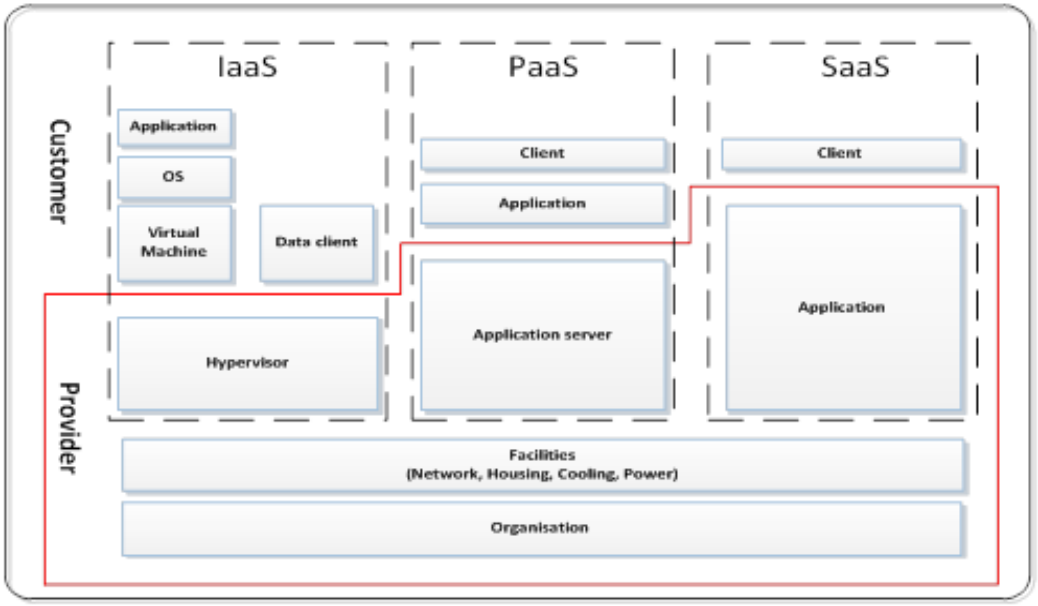
- infrastruktura jako usługa (IaaS): kategoria usług w chmurze, w ramach której rodzajem zasobu w chmurze udostępnianego klientowi jest infrastruktura. Obejmuje ona wirtualne dostarczanie zasobów obliczeniowych w postaci sprzętu komputerowego, usług sieciowych i usług pamięci. Model IaaS jest wykorzystywany do obsługi serwerów, pamięci, sieci i systemów operacyjnych. Zapewnia on przedsiębiorstwom infrastrukturę umożliwiającą im przechowywanie danych i korzystanie z aplikacji, których potrzebują one w swojej codziennej działalności;

- platforma jako usługa (PaaS): kategoria usług w chmurze, w ramach której rodzajem zasobu w chmurze udostępnianego klientowi jest platforma. Obejmuje ona zapewnianie dostępu do internetowych platform obliczeniowych, które umożliwiają przedsiębiorstwom korzystanie z istniejących aplikacji lub opracowywanie i testowanie nowych aplikacji;

- oprogramowanie jako usługa (SaaS): kategoria usług w chmurze, w ramach której rodzajem zasobu w chmurze udostępnianego klientowi jest aplikacja lub oprogramowanie rozpowszechniane za pośrednictwem internetu. Tego rodzaju usługi w chmurze eliminują konieczność kupowania i instalowania oprogramowania oraz zarządzania nim przez użytkownika końcowego oraz przynoszą korzyść w postaci zapewnienia możliwości uzyskania dostępu do oprogramowania z dowolnego miejsca dysponującego połączeniem z internetem.

[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Instytut Technologii w Karlsruhe, „Elasticity in Cloud Computing: What It Is, What It Is Not", publikacja dostępna pod adresem: https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. Zob. również COM(2012) 529, ss. 2–5.

**Wykres 5: Modele usług i aktywa w przetwarzaniu w chmurze**




ENISA zapewniła kompleksowe wytyczne dotyczące konkretnych zagadnień związanych z chmurą obliczeniową[36] oraz wytyczne dotyczące podstawowych kwestii związanych z przetwarzaniem w chmurze[37].

### 4.4.2. Wymogi w zakresie bezpieczeństwa.

Zgodnie z art. 16 ust. 1 państwa członkowskie są zobowiązane do zapewnienia, aby dostawcy usług cyfrowych wprowadzali odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania zagrożeniami dla bezpieczeństwa sieci i systemów informatycznych, z których korzystają do świadczenia swoich usług. Wspomniane środki bezpieczeństwa powinny uwzględniać najnowszy stan wiedzy oraz następujących pięć elementów: (i) bezpieczeństwo systemów i obiektów; (ii) postępowanie w przypadku incydentu; (iii) zarządzanie ciągłością działania; (iv) monitorowanie, audyt i testowanie; (v) zgodność z normami międzynarodowymi.

W tym względzie zgodnie z art. 16 ust. 8 Komisja jest uprawniona do przyjmowania aktów wykonawczych doprecyzowujących te elementy i służących zapewnieniu wysokiego poziomu harmonizacji w odniesieniu do tych dostawców usług. Przewiduje się, że Komisja przyjmie stosowny akt wykonawczy jesienią 2017 r. Ponadto państwa członkowskie są zobowiązane do zapewnienia wprowadzania przez dostawców usług cyfrowych koniecznych środków zapobiegających występowaniu incydentów i minimalizujących ich wpływ w celu zagwarantowania ciągłości świadczonych przez nich usług.

[36] Dostępne pod adresem: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security
[37] ENISA, *Cloud Security Guide for SMEs* (2015 r.). Dostępne pod adresem: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

### 4.4.3. Wymogi dotyczące zgłaszania incydentów

Dostawcy usług cyfrowych powinni być zobowiązani do zgłaszania poważnych incydentów właściwym organom lub CSIRT. Zgodnie z art. 16 ust. 3 dyrektywy w sprawie bezpieczeństwa sieci i informacji dostawcy usług cyfrowych będą zobowiązani do zgłoszenia incydentu bezpieczeństwa w przypadku, gdy dany incydent bezpieczeństwa ma istotny wpływ na świadczenie usługi. Do celów związanych z określaniem istotności wpływu w art. 16 ust. 4 wymieniono w szczególności pięć parametrów, które dostawcy usług cyfrowych muszą wziąć pod uwagę. W tym względzie zgodnie z art. 16 ust. 8 Komisja jest uprawniona do przyjmowania aktów wykonawczych zawierających bardziej szczegółowe opisy tych parametrów. Parametry te zostaną doprecyzowane w akcie wykonawczym doprecyzowującym elementy bezpieczeństwa wymienione w pkt 4.4.2, który Komisja zamierza przyjąć jesienią.

### 4.4.4. Podejście regulacyjne oparte na analizie ryzyka

Art. 17 stanowi, że właściwe organy krajowe muszą poddawać dostawców usług cyfrowych kontroli nadzorczej *ex post*. Państwa członkowskie muszą zapewnić podjęcie stosownych działań przez właściwe organy w przypadku otrzymania dowodów świadczących o tym, że dostawca usług cyfrowych nie spełnia wymogów określonych w art. 16 dyrektywy.

Ponadto zgodnie z art. 16 ust. 8 i 9 Komisja jest uprawniona do przyjmowania aktów wykonawczych dotyczących wymogów w zakresie bezpieczeństwa i zgłaszania incydentów, które przyczynią się do zwiększenia poziomu harmonizacji dostawców usług cyfrowych. Ponadto zgodnie z art. 16 ust. 10 państwa członkowskie nie mogą nakładać na dostawców usług cyfrowych żadnych dodatkowych wymogów w zakresie bezpieczeństwa i zgłaszania incydentów poza wymogami przewidzianymi w dyrektywie, z wyjątkiem przypadków, w których nałożenie takich środków jest konieczne w celu zapewnienia ochrony ich podstawowych funkcji państwowych, w szczególności w celu zagwarantowania bezpieczeństwa narodowego oraz w celu umożliwienia prowadzenia postępowań przygotowawczych, wykrywania i ścigania przestępstw.

Ponadto, biorąc pod uwagę transgraniczny charakter działalności prowadzonej przez dostawców usług cyfrowych, w dyrektywie nie przewidziano modelu obejmującego wiele równoległych jurysdykcji – zamiast tego ustanowiono w niej kryterium głównej jednostki organizacyjnej przedsiębiorstwa na terytorium UE[38]. Zastosowanie tego podejścia umożliwia przyjęcie jednego zbioru zasad, które będą miały zastosowanie do dostawców usług cyfrowych, i wyznaczenie jednego właściwego organu odpowiedzialnego za sprawowanie nadzoru, co ma szczególnie istotne znaczenie z uwagi na fakt, że wielu dostawców usług cyfrowych świadczy swoje usługi w wielu państwach członkowskich jednocześnie. Zastosowanie tego podejścia ogranicza do minimum spoczywające na dostawcach usług cyfrowych obciążenia związane z koniecznością zapewnienia zgodności i zapewnia prawidłowe funkcjonowanie jednolitego rynku cyfrowego.

[38] Zob. w szczególności art. 18 dyrektywy.

### 4.4.5. Jurysdykcja

Jak wyjaśniono powyżej, zgodnie z art. 18 ust. 1 dyrektywy w sprawie bezpieczeństwa sieci i informacji dostawca usług cyfrowych podlega jurysdykcji państwa członkowskiego, w którym znajduje się jego główna jednostka organizacyjna. Jeżeli konkretny dostawca usług cyfrowych świadczy usługi w UE, ale jego główna jednostka organizacyjna nie znajduje się na terytorium UE, zgodnie z art. 18 ust. 2 taki dostawca usług cyfrowych ma obowiązek wyznaczyć swojego przedstawiciela w Unii. W takim przypadku dane przedsiębiorstwo podlega jurysdykcji państwa członkowskiego, w którym przedstawiciel posiada jednostkę organizacyjną. Jeżeli dostawca usług cyfrowych świadczy usługi w państwie członkowskim, ale nie wyznaczył swojego przedstawiciela w UE, państwo członkowskie może co do zasady podjąć działania prawne przeciwko takiemu dostawcy usług cyfrowych, ponieważ dostawca narusza spoczywające na nim obowiązki wynikające z dyrektywy.

### 4.4.6. Wyłączenie dostawców usług cyfrowych działających na niewielką skalę z zakresu obowiązywania wymogów w zakresie bezpieczeństwa i zgłaszania incydentów

Zgodnie z art. 16 ust. 11 dostawcy usług cyfrowych będący mikroprzedsiębiorstwami lub małymi przedsiębiorstwami w rozumieniu zalecenia Komisji 2003/361/WE39 są wyłączeni z zakresu wymogów w zakresie bezpieczeństwa i zgłaszania incydentów ustanowionych w art. 16. Oznacza to, że wymogi te nie mają zastosowania do przedsiębiorstw zatrudniających mniej niż 50 osób, których obrót roczny lub których suma bilansowa nie przekracza 10 mln EUR. Przy ustalaniu wielkości podmiotu nie ma znaczenia, czy dane przedsiębiorstwo świadczy wyłącznie usługi cyfrowe w rozumieniu dyrektywy w sprawie bezpieczeństwa sieci i informacji czy też również innego rodzaju usługi.

## 5. Związek pomiędzy dyrektywą w sprawie bezpieczeństwa sieci i informacji a innymi aktami prawnymi

W niniejszym punkcie skoncentrowano się na zawartych w art. 1 ust. 7 dyrektywy w sprawie bezpieczeństwa sieci i informacji przepisach dotyczących przepisów szczególnych, przedstawiono trzy przykłady przepisów szczególnych, które Komisja do tej pory poddała ocenie, oraz wyjaśniono wymogi w zakresie bezpieczeństwa i zgłaszania incydentów mające zastosowanie do dostawców usług telekomunikacyjnych i dostawców usług zaufania.

### 5.1. Dyrektywa w sprawie bezpieczeństwa sieci i informacji, art. 1 ust. 7: stosowanie przepisów szczególnych

Zgodnie z art. 1 ust. 7 dyrektywy w sprawie bezpieczeństwa sieci i informacji przepisy dotyczące wymogów w zakresie bezpieczeństwa lub zgłaszania incydentów nałożonych na mocy dyrektywy na dostawców usług cyfrowych lub operatorów usług kluczowych nie mają zastosowania, jeżeli sektorowy akt prawny Unii przewiduje wymogi w zakresie bezpieczeństwa lub zgłaszania incydentów wywołujące skutek co najmniej równoważny skutkowi odpowiednich obowiązków nałożonych dyrektywą w sprawie bezpieczeństwa sieci

[39] Dz.U. L 24 z 20.5.2003, s. 36.

i informacji. Państwa członkowskie muszą uwzględnić art. 1 ust. 7 przy ogólnej transpozycji dyrektywy i przekazywać Komisji informacje o zastosowaniu przepisów szczególnych.

*Metodyka*

Oceniając równoważność sektorowego aktu prawnego Unii z odpowiednimi przepisami dyrektywy w sprawie bezpieczeństwa sieci i informacji, należy zwrócić szczególną uwagę na to, czy obowiązki w zakresie bezpieczeństwa przewidziane w sektorowym akcie prawnym obejmują środki zapewniające bezpieczeństwo sieci i systemów informatycznych zdefiniowane w art. 4 pkt 2 dyrektywy.

Jeżeli chodzi o wymogi dotyczące zgłaszania incydentów, zgodnie z art. 14 ust. 3 i art. 16 ust. 3 dyrektywy w sprawie bezpieczeństwa sieci i informacji operatorzy usług kluczowych i dostawcy usług cyfrowych muszą bez zbędnej zwłoki zgłaszać właściwym organom lub CSIRT wszelkie incydenty mające istotny/poważny wpływ na świadczenie usługi. W tym kontekście należy zwrócić szczególną uwagę na spoczywające na operatorze / dostawcy usług cyfrowych obowiązki dotyczące uwzględnienia w zgłoszeniu incydentu informacji umożliwiających właściwemu organowi lub CSIRT określenie transgranicznego wpływu incydentu.

Obecnie nie istnieje żadne prawodawstwo sektorowe mające zastosowanie do kategorii dostawców usług cyfrowych, w którym przewidziano by wymogi w zakresie bezpieczeństwa i zgłaszania incydentów porównywalne z wymogami ustanowionymi w art. 16 dyrektywy w sprawie bezpieczeństwa sieci i informacji i które można być uwzględnić przez stosowaniu przepisów art. 1 ust. 7 dyrektywy w sprawie bezpieczeństwa sieci i informacji[40].

Jeżeli chodzi o operatorów usług kluczowych, sektor finansowy, w szczególności sektory bankowości i infrastruktury rynków finansowych, o których mowa w pkt 3 i 4 załącznika II, podlegają obecnie wymogom w zakresie bezpieczeństwa lub zgłaszania incydentów zawartym w unijnym prawodawstwie sektorowym. Wynika to z faktu, że zagwarantowanie bezpieczeństwa i solidności struktury IT oraz sieci i systemów informatycznych wykorzystywanych przez instytucje finansowe stanowi kluczowy element wymogów w zakresie ryzyka operacyjnego nakładanych na instytucje finansowe na mocy prawa Unii.

*Przykłady*

**(i) Druga dyrektywa w sprawie usług płatniczych**

Jeżeli chodzi o sektor bankowy, w szczególności o świadczenie usług płatniczych przez instytucje kredytowe zdefiniowane w art. 4 pkt 1 rozporządzenia (UE) nr 575/2013, w tzw. drugiej dyrektywie w sprawie usług płatniczych (PSD 2)[41] przewidziano wymogi w zakresie bezpieczeństwa i zgłaszania incydentów, które ustanowiono w art. 95 i 96 tej dyrektywy.

[40] Pozostaje to bez uszczerbku dla możliwości zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu zgodnie z art. 33 ogólnego rozporządzenia o ochronie danych.
[41] Dyrektywa (UE) 2015/2366, Dz.U. L 337 z 23.12.2015, s. 35.

Ściślej rzecz biorąc, w art. 95 ust. 1 tej dyrektywy na dostawców usług płatniczych nałożono obowiązek przyjmowania odpowiednich środków ograniczających ryzyko i mechanizmów kontroli, które pozwolą zarządzać ryzykami operacyjnymi oraz ryzykami dla bezpieczeństwa, związanymi z usługami płatniczymi świadczonymi przez tych dostawców. Środki te powinny zapewniać ustanowienie i utrzymanie skutecznych procedur zarządzania incydentami, uwzględniając procedury umożliwiające wykrywanie i klasyfikację poważnych incydentów operacyjnych i incydentów związanych z bezpieczeństwem. W motywach 95 i 96 drugiej dyrektywy w sprawie usług płatniczych doprecyzowano charakter takich środków bezpieczeństwa. Z treści tych przepisów wynika jasno, że środki te służą zarządzaniu zagrożeniami dla bezpieczeństwa związanymi z siecią i systemami informatycznymi wykorzystywanymi do świadczenia usług płatniczych. Dlatego też można uznać, że wymogi w zakresie bezpieczeństwa wywierają skutek co najmniej równoważny skutkowy wywieranemu przez odpowiadające im przepisy zawarte w art. 14 ust. 1 i 2 dyrektywy w sprawie bezpieczeństwa sieci i informacji.

Jeżeli chodzi o wymogi dotyczące zgłaszania incydentów, w art. 96 ust. 1 drugiej dyrektywy w sprawie usług płatniczych na dostawców usług płatniczych nałożono obowiązek zgłaszania właściwemu organowi poważnych incydentów bezpieczeństwa bez zbędnej zwłoki. Ponadto, podobnie jak art. 14 ust. 5 dyrektywy w sprawie bezpieczeństwa sieci i informacji, w art. 96 ust. 2 drugiej dyrektywy w sprawie usług płatniczych na właściwy organ nałożono obowiązek przekazania stosownych informacji na temat incydentu właściwym organom innych państw członkowskich, jeżeli dany incydent jest istotny z ich punktu widzenia. Obowiązek też oznacza również, że zgłoszenie incydentów bezpieczeństwa musi zawierać informacje umożliwiające organom ocenę transgranicznego wpływu incydentu. W art. 96 ust. 3 lit. a) drugiej dyrektywy w sprawie usług płatniczych upoważniono EUNB działający we współpracy z EBC do opracowywania szczegółowych wytycznych dotyczących treści i formatu zgłoszenia.

W rezultacie można stwierdzić, że zgodnie z art. 1 ust. 7 dyrektywy w sprawie bezpieczeństwa sieci i informacji w kwestiach związanych ze świadczeniem usług płatniczych przez instytucje kredytowe zamiast odpowiednich wymogów przewidzianych w art. 14 dyrektywy w sprawie bezpieczeństwa sieci i informacji zastosowanie powinny mieć wymogi w zakresie bezpieczeństwa i zgłaszania incydentów ustanowione w art. 95 i 96 drugiej dyrektywy w sprawie usług płatniczych.

**(ii) 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**

Jeżeli chodzi o infrastrukturę rynku finansowego, rozporządzenie (UE) nr 648/2012, w związku z rozporządzeniem delegowanym Komisji (UE) nr 153/2013, zawiera przepisy dotyczące wymogów w zakresie bezpieczeństwa spoczywających na kontrahentach centralnych (CCP), które można uznać za przepisy szczególne. We wspomnianych aktach prawnych przewidziano w szczególności środki techniczne i organizacyjne dotyczące bezpieczeństwa sieci i systemów informatycznych, które są jeszcze bardziej szczegółowe niż

wymogi zawarte w art. 14 ust. 1 i 2 dyrektywy w sprawie bezpieczeństwa sieci i informacji i które można tym samym uznać za spełniające wymogi art. 1 ust. 7 dyrektywy w sprawie bezpieczeństwa sieci i informacji w zakresie, w jakim dotyczą wymogów w zakresie bezpieczeństwa.

Ściślej rzecz biorąc, art. 26 ust. 1 rozporządzenia (UE) nr 648/2012 stanowi, że dany podmiot powinien posiadać „solidne zasady zarządzania obejmujące jasną strukturę organizacyjną z dobrze określonymi, przejrzystymi i spójnymi obszarami odpowiedzialności, skuteczne procesy służące rozpoznawaniu ryzyka, na które jest lub może być narażony CCP, zarządzaniu ryzykiem, monitorowaniu i zgłaszaniu ryzyka oraz odpowiednie mechanizmy kontroli wewnętrznej obejmujące prawidłowe procedury administracyjne i rachunkowości". W art. 26 ust. 3 na strukturę organizacyjną nałożono wymóg zapewnienia ciągłości działania, prawidłowego świadczenia usług i podejmowania działań za pomocą odpowiednich i proporcjonalnych systemów, zasobów i procedur.

Ponadto w art. 26 ust. 6 wyjaśniono, że CCP jest zobowiązany do posiadania „odpowiednich systemów informatycznych pozwalających na uwzględnienie złożoności, różnorodności i rodzaju świadczonych usług oraz prowadzonej działalności, tak aby zapewnić wysokie standardy bezpieczeństwa oraz integralność i poufność informacji". Ponadto w art. 34 ust. 1 przewidziano wymóg ustanowienia, wprowadzenia i utrzymania odpowiedniej strategii na rzecz ciągłości działania oraz planu przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej, które powinny zapewnić szybkie przywrócenie działalności.

Obowiązki w tym zakresie zostały doprecyzowane w rozporządzeniu delegowanym Komisji (UE) nr 153/2013 z dnia 19 grudnia 2012 r. uzupełniającym rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 w odniesieniu do regulacyjnych standardów technicznych dotyczących wymogów obowiązujących kontrahentów centralnych[42]. W szczególności w art. 4 tego rozporządzenia delegowanego na kontrahentów centralnych nałożono wymóg opracowania odpowiednich narzędzi zarządzania ryzykiem, aby mogli oni zarządzać wszystkimi istotnymi rodzajami ryzyka oraz składać na ich temat sprawozdania, i doprecyzowano rodzaje środków (np.: stosowanie solidnych systemów informacyjnych i systemów kontroli ryzyka, dostępność środków i wiedzy fachowej dla funkcji zarządzania ryzykiem oraz posiadanie przez nią dostępu do wszelkich istotnych informacji, dostępność odpowiednich mechanizmów kontroli wewnętrznej takich jak prawidłowe procedury administracyjne i rachunkowości ułatwiające zarządowi CCP monitorowanie i ocenę adekwatności i skuteczności jego polityk, procedur i systemów zarządzania ryzykiem).

Ponadto w art. 9 odniesiono się wprost do problematyki związanej z bezpieczeństwem systemów informatycznych i wprowadzono konkretne środki techniczne i organizacyjne związane z utrzymaniem solidnych ram bezpieczeństwa informacyjnego do celów zarządzania zagrożeniami dla bezpieczeństwa informatycznego. Środki takie powinny obejmować mechanizmy i procedury zapewniające dostępność usług oraz ochronę autentyczności, integralności i poufności danych.

[42] Dz.U. L 52 z 23.2.2013, s. 41.

**(iii) 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[43]**

Jeżeli chodzi o systemy obrotu, w art. 48 ust. 1 dyrektywy 2014/65/UE na operatorów nałożono wymóg zapewnienia ciągłości świadczenia swoich usług w przypadku wystąpienia jakichkolwiek awarii ich systemów transakcyjnych. Ten ogólny obowiązek został niedawno doprecyzowany i uzupełniony rozporządzeniem delegowanym Komisji (UE) 2017/584[44] z dnia 14 lipca 2016 r. uzupełniającym dyrektywę Parlamentu Europejskiego i Rady 2014/65/UE w odniesieniu do regulacyjnych standardów technicznych określających wymogi organizacyjne w zakresie systemów obrotu[45]. W szczególności art. 23 ust. 1 tego rozporządzenia stanowi, że systemy obrotu dysponują procedurami i mechanizmami w zakresie bezpieczeństwa fizycznego i elektronicznego opracowanymi w celu ochrony ich systemów przed nadużyciami lub nieuprawnionym dostępem oraz dla zapewnienia integralności danych. Środki te powinny umożliwiać zapobieganie ryzyku lub ograniczanie ryzyka ataków na systemy informatyczne.

Ponadto w art. 23 ust. 2 ustanowiono wymóg, zgodnie z którym podejmowane przez operatorów środki i mechanizmy powinny zapewniać możliwość szybkiego identyfikowania ryzyka związanego z nieuprawnionym dostępem, wszelkimi ingerencjami w system, które poważnie naruszają lub przerywają funkcjonowanie systemów informacyjnych, oraz wszelkimi ingerencjami w dane wywierającymi niekorzystny wpływ na ich dostępność, integralność lub autentyczność, a także zarządzania takim ryzykiem. Ponadto w art. 15 rozporządzenia systemy obrotu zobowiązano do przyjęcia skutecznych rozwiązań w zakresie ciągłości działania, aby zagwarantować stabilność systemu i rozwiązać problemy związane z zakłóceniami. Środki takie powinny w szczególności umożliwić operatorowi wznowienie obrotu w ciągu dwóch godzin lub około dwóch godzin, gwarantując jednocześnie ograniczenie ilości utraconych danych niemal do zera.

W art. 16 stwierdzono ponadto, że zidentyfikowane środki służące rozwiązywaniu problemów związanych z zakłóceniami i zarządzaniu zakłóceniami powinny stanowić jeden z elementów planu ciągłości działania systemów obrotu i powinny zawierać konkretne elementy, które operator musi wziąć pod uwagę przy przyjmowaniu planu ciągłości działania (np. powołanie specjalnego zespołu ds. operacji w zakresie bezpieczeństwa, przeprowadzanie oceny skutków służącej zidentyfikowaniu czynników ryzyka i poddawanie tej oceny okresowemu przeglądowi).

Biorąc pod uwagę treść tych środków bezpieczeństwa, wydaje się, że mają one służyć zarządzaniu ryzykiem związanym z dostępnością, autentycznością, integralnością i poufnością danych lub świadczonych usług i rozwiązywaniu problemów związanych z tym ryzykiem; w rezultacie można stwierdzić, że wspomniany powyżej sektorowy akt prawny

[43] Dz.U. L 173 z 12.6.2014, s. 349.
[44] Dz.U. L 87 z 31.3.2017, s. 350.
[45] http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_en.pdf

Unii zawiera zobowiązania w zakresie bezpieczeństwa wywierające skutki co najmniej równoważne skutkom odpowiednich zobowiązań przewidzianych w art. 14 ust. 1 i 2 dyrektywy w sprawie bezpieczeństwa sieci i informacji.

### 5.2. Dyrektywa w sprawie bezpieczeństwa sieci i informacji, art. 1 ust. 3: dostawcy usług telekomunikacyjnych i dostawcy usług zaufania

Zgodnie z art. 1 ust. 3 wymogi w zakresie bezpieczeństwa i zgłaszania incydentów przewidziane w dyrektywie nie mają zastosowania do dostawców, którzy podlegają wymogom art. 13a i 13b dyrektywy 2002/21/WE. Przepisy art. 13a i 13b dyrektywy 2002/21/WE mają zastosowanie do przedsiębiorstw udostępniających publiczne sieci łączności lub świadczących publicznie dostępne usług łączności elektronicznej. W rezultacie, jeżeli chodzi o udostępnianie publicznych sieci łączności lub świadczenie publicznie dostępnych usług łączności elektronicznej, przedsiębiorstwa muszą spełnić wymogi w zakresie bezpieczeństwa i zgłaszania incydentów przewidziane w dyrektywie 2002/21/WE.

Jeżeli jednak to samo przedsiębiorstwo świadczy również inne usługi takie jak usługi cyfrowe (np. usługi przetwarzania w chmurze lub usługi związane z internetową platformą handlową) wymienione w załączniku III do dyrektywy w sprawie bezpieczeństwa sieci i informacji lub usługi takie jak usługi w zakresie DNS lub IXP, o których mowa w pkt 7 załącznika II do dyrektywy w sprawie bezpieczeństwa sieci i informacji, przedsiębiorstwo takie będzie podlegało wymogom w zakresie bezpieczeństwa i zgłaszania incydentów przewidzianym w dyrektywie w sprawie bezpieczeństwa sieci i informacji przy świadczeniu tych konkretnych usług. Należy podkreślić, że z uwagi na fakt, iż dostawcy usług wymienionych w załączniku II pkt 7 należą do kategorii operatorów usług kluczowych, państwa członkowskie są zobowiązane przeprowadzić proces identyfikacji zgodnie z art. 5 ust. 2 i zidentyfikować tych indywidualnych dostawców usług w zakresie DNS, IXP lub TLD, którzy powinni zostać objęci wymogami dyrektywy w sprawie bezpieczeństwa sieci i informacji. Oznacza to, że po przeprowadzeniu takiej oceny wymogi dyrektywy w sprawie bezpieczeństwa sieci i informacji będą miały zastosowanie wyłącznie do tych dostawców usług w zakresie DNS, IXP lub TLD, którzy spełnią kryteria przewidziane w art. 5 ust. 2 tej dyrektywy.

Art. 1 ust. 3 stanowi ponadto, że przewidziane w dyrektywie wymogi w zakresie bezpieczeństwa i zgłaszania incydentów nie mają zastosowania do dostawców usług zaufania, którzy podlegają podobnym wymogom ustanowionym w art. 19 rozporządzenia (UE) nr 910/2014.

## 6. Opublikowane krajowe strategie bezpieczeństwa cybernetycznego

| | Państwo członkowskie | Tytuł strategii i dostępne linki |
|---|---|---|
| **1** | Austria | *Austriacka strategia bezpieczeństwa cybernetycznego* (2013 r.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN) |
| **2** | Belgia | *Ochrona cyberprzestrzeni* (2012 r.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR) |
| **3** | Bułgaria | *Bułgaria odporna na zagrożenia dla cyberbezpieczeństwa 2020* (2016 r.) http://www.cyberbg.eu/ (BG) |
| **4** | Chorwacja | *Krajowa strategia bezpieczeństwa cybernetycznego Republiki Chorwacji* (2015 r.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN) |
| **5** | Republika Czeska | *Krajowa strategia bezpieczeństwa cybernetycznego Republiki Czeskiej na lata 2015–2020* (2015 r.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN) |
| **6** | Cypr | *Strategia bezpieczeństwa cybernetycznego Republiki Cypryjskiej* (2012 r.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN) |
| **7** | Dania | *Duńska strategia bezpieczeństwa cybernetycznego i informatycznego* (2015 r.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN) |
| **8** | Estonia | *Strategia bezpieczeństwa cybernetycznego* (2014 r.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN) |
| **9** | Finlandia | *Strategia bezpieczeństwa cybernetycznego Finlandii* (2013 r.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN) |
| **10** | Francja | *Francuska krajowa strategia bezpieczeństwa cyfrowego* (2015 r.) |

| | | |
|---|---|---|
| | | https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN) |
| **11** | Irlandia | *Krajowa strategia bezpieczeństwa cybernetycznego na lata 2015–2017* (2015 r.)<br>https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN) |
| **12** | Włochy | *Krajowe ramy strategiczne na rzecz bezpieczeństwa cyberprzestrzeni* (2013 r.)<br>https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN) |
| **13** | Niemcy | *Strategia bezpieczeństwa cybernetycznego dla Niemiec* (2016 r.)<br>http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE) |
| **14** | Węgry | *Krajowa strategia bezpieczeństwa cybernetycznego Węgier* (2013 r.)<br>https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN) |
| **15** | Łotwa | *Strategia bezpieczeństwa cybernetycznego Łotwy na lata 2014–2018* (2014 r.)<br>https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN) |
| **16** | Litwa | *Program na rzecz zwiększania bezpieczeństwa informacji elektronicznych (bezpieczeństwa cybernetycznego) na lata 2011–2019* (2011 r.)<br>https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN) |
| **17** | Luksemburg | *Druga krajowa strategia bezpieczeństwa cybernetycznego* (2015 r.)<br>https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN) |
| **18** | Malta | *Zielona księga dotycząca krajowej strategii bezpieczeństwa cybernetycznego* (2015 r.)<br>https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN) |
| **19** | Niderlandy | *Druga krajowa strategia bezpieczeństwa cybernetycznego* (2013 r.)<br>https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN) |
| **20** | Polska | *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej* (2013 r.)<br>https://www.enisa.europa.eu/topics/national-cyber-security- |

| | | |
|---|---|---|
| | | strategies/ncss-map/copy_of_PO_NCSS.pdf (EN) |
| **21** | Rumunia | *Strategia bezpieczeństwa cybernetycznego Rumunii* (2011 r.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO) |
| **22** | Portugalia | *Krajowa strategia bezpieczeństwa cyberprzestrzeni* (2015 r.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/portuguese-national-cyber-security-strategy/view (EN) |
| **23** | Republika Słowacka | *Koncepcja bezpieczeństwa cybernetycznego Republiki Słowackiej na lata 2015–2020* (2015 r.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN) |
| **24** | Słowenia | *Strategia bezpieczeństwa cybernetycznego ustanawiająca system zapewniania wysokiego poziomu bezpieczeństwa cybernetycznego* (2016 r.) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN) |
| **25** | Hiszpania | *Krajowa strategia bezpieczeństwa cybernetycznego* (2013 r.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN) |
| **26** | Szwecja | *Szwedzka krajowa strategia bezpieczeństwa cybernetycznego* (2017 r.) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN) |
| **27** | Zjednoczone Królestwo | *Krajowa strategia bezpieczeństwa cybernetycznego (na lata 2016–2021)* (2016 r.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN) |

## 7. Wykaz publikacji ENISA zawierających dobre praktyki i zalecenia

Publikacje dotyczące reagowania na incydenty

- ✓ Strategie w zakresie reagowania na incydenty i współpracy na wypadek kryzysów w cyberprzestrzeni[46]

Publikacje dotyczące postępowania w przypadku incydentu

- ✓ Projekt automatyzacji postępowania w przypadku incydentu[47]
- ✓ Podręcznik dobrych praktyk w zakresie zarządzania incydentami[48]

Publikacje dotyczące klasyfikacji i taksonomii incydentów

- ✓ Przegląd istniejących taksonomii[49]
- ✓ Podręcznik dobrych praktyk w zakresie wykorzystywania taksonomii do celów zapobiegania incydentom i ich wykrywania[50]

Publikacje dotyczące dojrzałości CSIRT

- ✓ Wyzwania stojące przed krajowymi CSIRT w Europie w 2016 r.: badanie dotyczące dojrzałości CSIRT[51]
- ✓ Badanie dotyczące dojrzałości CSIRT – proces oceny[52]
- ✓ Wytyczne dla krajowych i rządowych CSIRT dotyczące sposobu oceny stopnia dojrzałości[53]

Publikacje dotyczące budowania zdolności i szkolenia CSIRT

- ✓ Podręcznik dobrych praktyk w zakresie metod szkoleniowych[54]

Dodatkowe informacje na temat CSIRT istniejących w Europie – Przegląd CSIRT z podziałem na państwa[55]

---

[46] ENISA, *Strategies for incident response and cyber crisis cooperation* (2016 r.). Dokument dostępny pod adresem:https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation
[47] Więcej informacji można uzyskać pod adresem: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation
[48] ENISA, *Good Practice Guide for Incident Management* (2010 r.). Dokument dostępny pod adresem:https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
[49] Więcej informacji można uzyskać pod adresem: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies
[50] ENISA, *A good practice guide of using taxonomies in incident prevention and detection* (2017 r.). Dokument dostępny pod adresem:https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection
[51] ENISA, *Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity* (2017 r.). Dokument dostępny pod adresem:https://www.enisa.europa.eu/publications/study-on-csirt-maturity
[52] ENISA, *Study on CSIRT Maturity – Evaluation Process* (2017 r.). Dokument dostępny pod adresem:https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process
[53] ENISA, CSIRT Capabilities. *How to assess maturity? Guidelines for national and governmental CSIRTs* (2016 r.). Dokument dostępny pod adresem: https://www.enisa.europa.eu/publications/csirt-capabilities
[54] ENISA, *Good Practice Guide on Training Methodologies* (2014 r.). Dokument dostępny pod adresem:https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies

[55] Więcej informacji można uzyskać pod adresem: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map