PROJEKT STANOWISKA RP

przygotowany w związku z art. 7 ustawy z dnia 8 października 2010 r. o współpracy Rady Ministrów z Sejmem i Senatem w sprawach związanych z członkostwem Rzeczypospolitej Polskiej w Unii Europejskiej (Dz. U. Nr 213, poz. 1395)

Dotyczy	Wniosek Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylająca dyrektywę (UE) 2016/1148

Data przekazania Polsce dokumentu przez instytucje UE	19 stycznia 2021 r.

Sygnatura dokumentu	Komisja Europejska	COM(2020)823
	Numer międzyinstytucjonalny	2020/0359(COD)

Procedura decyzyjna	Zwykła procedura ustawodawcza

Tryb głosowania w Radzie UE	Większość kwalifikowana

Instytucja wiodąca	Kancelaria Prezesa Rady Ministrów

Instytucje współpracujące	Ministerstwo Klimatu i Środowiska Ministerstwo Zdrowia Ministerstwo Obrony Narodowej Ministerstwo Infrastruktury Urząd Komisji Nadzoru Finansowego Ministerstwo Spraw Zagranicznych Ministerstwo Spraw Wewnętrznych i Administracji

Data przyjęcia przez KSE	…. lutego 2021 r.

I. Cel projektu aktu prawnego

Projekt ma na celu wprowadzenie nowych środków zwiększających odporność i zdolności reagowania na incydenty cyberbezpieczeństwa. Osiągnięcie celu ma nastąpić między innymi poprzez zwiększenie liczby podmiotów objętych wspólnym (europejskim) systemem cyberbezpieczeństwa. Poprawienie działania w tym obszarze jest zgodne z unijnym celem dostosowania Europy do ery cyfrowej. Jednocześnie w związku z wyzwaniami przed jakimi stoi UE w dobie cyfryzacji, Komisja Europejska ogłosiła, tzw. Pakiet Cyberbezpieczeństwa. W jego skład, oprócz nowej Strategii Cyberbezpieczeństwa UE, wchodzi także projekt nowej dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (tzw. dyrektywa NIS2[1]), która uchyli obecnie obowiązującą dyrektywę NIS[2]. Ewaluacja dyrektywy w obecnym kształcie zidentyfikowała potencjalne obszary wymagające poprawy takie, jak:

- niski poziom cyberbezpieczeństwa firm działających w UE;
- niespójny poziom cyberbezpieczeństwa wśród państw członkowskich;
- niski poziom wspólnej świadomości sytuacyjnej i brak wspólnego reagowania kryzysowego.

Dyrektywa NIS2 modernizuje istniejący już system, mając na uwadze niedostatki dotychczasowej dyrektywy oraz trendy, które jeszcze bardziej nasiliły się w wyniku pandemii COVID-19 i jej następstw, tj. coraz większy poziom cyfryzacji rynku wewnętrznego i ewoluujący krajobraz zagrożeń cyberbezpieczeństwa, w tym wzrost liczby cyberataków. Projekt nowej dyrektywy stanowi odpowiedź na te wyzwania poprzez rozbudowanie dotychczasowej regulacji dyrektywy NIS o:

- dodanie nowych sektorów w oparciu o ich ważność dla funkcjonowania gospodarki i społeczeństwa;
- wprowadzenie nowego sposobu klasyfikacji podmiotów objętych zakresem dyrektywy;
- wzmocnienie wymogów w zakresie cyberbezpieczeństwa, które będą musiały zostać wdrożone przez podmioty objęte regulacjami;
- wprowadzenie szczegółowych przepisów dotyczących procesu zgłaszania incydentów, treści sprawozdań i terminów;
- wprowadzenie dla niektórych przedsiębiorstw wymogu przeciwdziałania zagrożeniom cyberbezpieczeństwa w łańcuchach dostaw i w relacjach z dostawcami (w szczególności chodzi o wzmocnienie cyberbezpieczeństwa w łańcuchach dostaw w obszarze kluczowych technologii informacyjnych i komunikacyjnych);
- wzmocnienie środków nadzorczych dla organów krajowych i harmonizacja systemu sankcji we wszystkich państwach członkowskich;
- zwiększenie roli Grupy Współpracy w kształtowaniu strategicznych decyzji politycznych oraz zwiększenie wymiany informacji i współpracy między organami państw członkowskich, a także wzmocnienie współpracy operacyjnej, w tym w zakresie zarządzania kryzysowego w obszarze cyberbezpieczeństwa;

[1] Wniosek Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylająca dyrektywę (UE) 2016/1148, COM/2020/823

[2] 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

- ustanowienie podstawowych ram w zakresie skoordynowanego ujawniania informacji na temat nowo wykrytych luk w zabezpieczeniach w całej UE oraz utworzenia rejestru UE prowadzonego przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (dalej ENISA).

II. Stanowisko RP

1. Rząd Rzeczypospolitej Polskiej (dalej: Rząd RP) stoi na stanowisku, że dyrektywa NIS2 powinna być podstawową regulacją horyzontalną, ustanawiającą wspólne, podstawowe i co do zasady niezmienne ramy funkcjonowania systemu cyberbezpieczeństwa, w tym w szczególności wymagania cyberbezpieczeństwa i ramy instytucjonalne zgłaszania incydentów oraz wsparcia w ich obsłudze. Regulacje dyrektywy NIS mogą być uzupełniane i doprecyzowywane w regulacjach sektorowych z uwagi na konieczność uwzględnienia specyfiki danego sektora oraz dojrzałości w budowaniu zdolności w zakresie cyberbezpieczeństwa. Równocześnie jednak regulacje sektorowe nie powinny zmieniać istoty i podstawowych zasad funkcjonowania systemu cyberbezpieczeństwa przewidzianych w NIS, w tym m.in. jednorodnego systemu raportowania incydentów, wymagań bezpieczeństwa oraz ram współpracy organów właściwych. Należy unikać fragmentaryzacji regulacji w obszarze cyberbezpieczeństwa oraz podejścia silosowego. Rząd RP stoi na stanowisku, że niezbędny jest spójny system zgłaszania incydentów na poziomie europejskim. Regulacje sektorowe nie powinny wprowadzać odmiennych procedur i definicji.

2. Rząd RP z zadowoleniem przyjmuje decyzję Komisji Europejskiej o rewizji dyrektywy NIS w formie prawnej dyrektywy.

3. Rząd RP popiera rozszerzenie zakresu dyrektywy NIS2 na sektory wymienione w załączniku I i II do projektu. Niezbędne jest przy tym zapewnienie, by zakres ten został ustalony w sposób jednoznaczny i precyzyjny, w szczególności z uwagi na przyjęty model określania podmiotów objętych zakresem dyrektywy.

4. Rząd RP z zadowoleniem przyjął propozycję KE włączenia administracji publicznej jako jednego z sektorów objętych regulacją.

5. Rząd RP przychyla się do propozycji KE dotyczącej podziału podmiotów na kluczowe (essential) oraz ważne (important) oraz przyjęcia reguły, że o objęciu regulacją dyrektywy decyduje fakt zakwalifikowania się do jednego z typów podmiotów z załącznika I albo II do projektu. Jednakże, Rząd RP widzi również potrzebę dalszej debaty nad mechanizmem wyznaczania podmiotów kluczowych i ważnych, w tym dyskusji na temat możliwości wprowadzenia dodatkowych kryteriów. Rząd RP popiera wyłączenie mikro i małych przedsiębiorstw z zakresu dyrektywy, dostrzegając jednak potrzebę wskazania w dyrektywie wyjątków w tym zakresie. Konieczne jest precyzyjne sformułowanie przepisów dyrektywy w tym zakresie.

6. Rząd RP popiera propozycje KE zawartą w art. 24 projektu, aby jurysdykcję dla dostawców usług DNS, rejestr nazw TLD, dostawców usług w chmurze, dostawców usług ośrodka przetwarzania danych oraz dostawców sieci dostarczania treści, o których mowa w załączniku I pkt 8 oraz dostawców usług cyfrowych, o których mowa w załączniku II pkt 6

ustalać co do zasady zgodnie z miejscem, w którym znajduje się ich główna jednostka organizacyjna w Unii.

7. Rząd RP dostrzega potrzebę dyskusji odnośnie propozycji utworzenia rejestru, o którym mowa w art. 25 projektu, w tym wyjaśnienie celu tego rejestru oraz roli ENISA.

8. Rząd RP popiera propozycję KE dotyczącą powiązania zarządzania kryzysowego z systemem cyberbezpieczeństwa (art.7), przy czym należy dążyć do spójności rozwiązań z projektem dyrektywy w sprawie odporności podmiotów krytycznych[3], w tym zapewnienia, że nie dojdzie do duplikowania zadań i kompetencji.

Rząd RP wielokrotnie zwracał uwagę na fakt, że obecne zapisy dyrektywy NIS pozwalały na szeroką współpracę pomiędzy państwami członkowskimi również w sytuacjach dotyczących incydentów transgranicznych czy obejmujących wiele krajów Unii jednocześnie. Z tego punktu widzenia istotne jest, aby nowy mechanizm współpracy CyCLONe[4], opisany w art. 14 projektu, nie powielał zadań już istniejących struktur (Sieć CSIRT i Grupa Współpracy NIS), a był w stosunku do nich komplementarny. Rząd RP zgadza się z propozycją zawartą w dyrektywie NIS2 odnośnie ustanowienia stałej i ustrukturyzowanej współpracy pomiędzy Grupą Współpracy NIS a odpowiednimi organami właściwymi utworzonymi w zakresie infrastruktury krytycznej w proponowanej przez KE dyrektywie w sprawie odporności podmiotów krytycznych, czy rozporządzeniu w sprawie cyfrowej odporności operacyjnej sektora finansowego (dalej DORA[5]).

9. Rząd RP stoi na stanowisku, że kary wymierzane podmiotom objętym zakresem dyrektywy za niewypełnienie nałożonych obowiązków w zakresie cyberbezpieczeństwa powinny być odstraszające, ale równocześnie motywujące i proporcjonalne.

10. Rząd RP przychylnie odnosi się do propozycji KE dotyczącej wprowadzenia europejskiego rejestru podatności (art. 6 projektu), jednakże należy wyjaśnić i doprecyzować zasady prowadzenia i funkcjonowania rejestru, w tym zakres danych w nim ujętych oraz zasady dostępu.

11. Rząd RP popiera przyjęcie odpowiednich przepisów w zakresie bezpieczeństwa łańcucha dostaw. Należy jednak zauważyć, że proponowane rozwiązania nakładają nowe obowiązki nie tylko dla podmiotów kluczowych i ważnych związane z zapewnieniem bezpieczeństwa łańcucha dostaw, ale także powodują nowe obowiązki w tym zakresie dla zespołów CSIRT[6].

12. Rząd RP z zadowoleniem przyjmuje propozycję KE dotyczącą zmian w regulacji i nadzorze nad dostawcami usług cyfrowych. Sektor ten jest jednym z kluczowych w dobie cyfryzacji usług, gdyż, jak wskazują analizy, wielu operatorów usług kluczowych przy świadczeniu swoich usług wykorzystuje systemy i usługi świadczone przez tych dostawców.

[3] Wniosek Dyrektywa Parlamentu Europejskiego i Rady UE w sprawie odporności podmiotów krytycznych COM / 2020/829

[4] CyCLONe - Cyber Crisis Liaison Organisation Network (Sieć Łącznikowa ds. Cyberzagrożeń)

[5] Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie cyfrowej odporności operacyjnej sektora finansowego oraz zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 i (UE) Nr 909/2014 COM/ 2020/595

[6] CSIRT – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego

13. Rząd RP stoi na stanowisku, że proponowana w art. 16 projektu regulacja w zakresie wzajemnego systemu oceny i sprawdzania (peer review) wymaga pogłębionej dyskusji, doprecyzowania i uzasadnienia jej celu oraz wartości dodanej.

14. Rząd RP popiera wzmocnienie kompetencji organów właściwych oraz rozszerzenie zadań CSIRT.

15. Rząd RP popiera zmiany w zakresie obowiązków raportowania wynikające z art. 20, w szczególności wprowadzenie dwustopniowego procesu zgłaszania incydentów, oraz obowiązku zespołu CSIRT poziomu krajowego zapewnienia wstępnej odpowiedzi na zgłoszenie incydentu. Rząd RP podkreśla konieczność przyjęcia ujednoliconych informacji o incydentach i zagrożeniach w państwach członkowskich, tak aby możliwe było przedstawienie wiarygodnego obrazu cyberbezpieczeństwa w UE.

16. Rząd popiera wprowadzenie regulacji dotyczących rejestru TLD[7], o którym mowa w art. 23 projektu.

17. Rząd RP pozytywnie odnosi się do propozycji dotyczących wykorzystania certyfikacji i standaryzacji w obszarze cyberbezpieczeństwa.

18. Rząd RP przychylnie odnosi się do propozycji dotyczącej porozumień w zakresie dzielenia się informacjami w obszarze cyberbezpieczeństwa (art. 26 projektu), przy czym propozycja ta wymaga szczegółowego wyjaśnienia i doprecyzowania.

19. Rząd RP popiera włączenie w ramy ustanowione w NIS zgłaszania incydentów na podstawie rozporządzenia 910/2014 (e-IDAS) oraz dyrektywy 2018/1972 (EKŁE) Przy czym pogłębionej analizy wymaga zakres zmian koniecznych w tych aktach dla zapewnienia spójności przyjętych rozwiązań w szczególności w zakresie nadzoru.

III. Uzasadnienie stanowiska RP

1. Rząd RP z zadowoleniem przyjął informację o rozpoczęciu przez Komisję Europejską w połowie 2020 r. procesu rewizji dyrektywy 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, a następnie o decyzji dokonania w niej zmian.
Dyrektywa NIS2 powinna być regulacją horyzontalną na poziomie europejskim w zakresie cyberbezpieczeństwa. Regulacje sektorowe powinny być tworzone w duchu komplementarności z dyrektywą NIS, nie powodując duplikowania obowiązków nakładanych na podmioty. Należy zwrócić uwagę, że obecnie procedowanych jest wiele projektów aktów prawnych, które w znacznej części dotyczą tych samych podmiotów, m.in.: Digital Services

[7] TLD – (Top Level Domain) - to ostatni segment nazwy domeny, czyli element znajdujący się po ostatniej kropce. Określa on obszar działalności (np. .org) lub obszar geograficzny (np. .pl) związanej z nią strony internetowej. Najpopularniejszym TLD jest bezapelacyjnie rozszerzenie .com.

Act[8], Digital Markets Act[9], Digital Operational Resilience Act[10], Data Governance Act[11], Directive on the resilience of critical entities[12]. Wiele z tych aktów zawiera definicje np. incydentu lub proponuje wdrożenie różnych procedur w sytuacji obsługi incydentów.

Rząd RP stanowczo podkreśla, że dyrektywa NIS2 powinna mieć horyzontalny charakter, a regulacje sektorowe powinny bazować na generalnych zasadach z niej wynikających. Tym samym, należy precyzyjnie określić stosowanie zasady lex specialis, pozwalającej na wyłączenia sektorowe zasad wynikających z NIS. Należy zatem zadbać, by regulacje sektorowe, jak DORA w sektorze finansowym, nie skutkowały wyłączeniem kluczowych zasad z NIS zapewniających kompleksowe cyberbezpieczeństwo. Jednocześnie zapisy w dyrektywie NIS2, powinny być przejrzyste i jasno określać, jakie sektory i podmioty są objęte zakresem NIS2 i w jakim zakresie są regulowane. Fragmentaryzacja regulacji w obszarze cyberbezpieczeństwa skutkuje obniżeniem zdolności podejmowania kompleksowych działań niezbędnych do zapewnienia wysokiego poziomu cyberbezpieczeństwa sieci i systemów informacyjnych.

2. Rząd RP aktywnie uczestniczył w pracach związanych z przeglądem dyrektywy NIS. Polska, jako pierwsze z państw członkowskich, przesłała Komisji Europejskiej postulaty w zakresie przeglądu dyrektywy NIS – w 14-punktowym dokumencie Rząd RP opowiadał się za zwiększeniem znaczenia dyrektywy NIS2 jako podstawowej, horyzontalnej regulacji w obszarze cyberbezpieczeństwa, dostrzegał potrzebę bardziej zharmonizowanego podejścia do dostawców usług cyfrowych, włączenia dostawców usług chmurowych do kategorii operatorów usług kluczowych, skoordynowanego podejścia w zakresie udostępniania informacji o podatnościach. Jednocześnie, Rząd RP wraz z 10 innymi państwami (Belgia, Bułgaria, Chorwacja, Czechy, Węgry, Irlandia, Łotwa, Litwa, Słowenia oraz Słowacja) w listopadzie 2020 r. wystosował do Komisji Europejskiej dokument (Non-paper on NIS regulatory framework), w którym podkreślono zasadność zachowania formy prawnej dyrektywy.

3. Rząd RP pozytywnie ocenia rozszerzenie dyrektywy na nowe sektory, podsektory lub typy podmiotów, określone w załącznikach I i II do projektu. Podkreślenia wymaga, że przepisy regulujące zakres dyrektywy muszą być jasne. Podmioty objęte zakresem dyrektywy powinny móc jednoznacznie określić czy mieszczą się w tym zakresie. Stąd też konieczna jest szczegółowa analiza przepisów, w tym załączników oraz dążenie do przyjęcia precyzyjnych przepisów. Szczególnej analizy wymaga sposób podziału dostawców usług cyfrowych na dwie kategorie. Należy przeprowadzić i omówić analizę potencjalnych nowych typów dostawców. Jednym z oczywistych kandydatów są platformy społecznościowe. Rząd RP pozytywnie ocenia przyjętą w dyrektywie zasadę minimalnej harmonizacji, która pozwala państwom

[8] Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie jednolitego rynku usług cyfrowych (ustawa o usługach cyfrowych) i zmieniająca dyrektywę 2000/31 / WE, COM / 2020/825

[9] Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie spornych i uczciwych rynków w sektorze cyfrowym (ustawa o rynkach cyfrowych), COM / 2020/842

[10] Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie cyfrowej odporności operacyjnej sektora finansowego oraz zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 i (UE) Nr 909/2014 COM / 2020/595

[11] Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie europejskiego zarządzania danymi (ustawa o zarządzaniu danymi), COM / 2020/767

[12] Wniosek Dyrektywa Parlamentu Europejskiego i Rady UE w sprawie odporności podmiotów krytycznych COM / 2020/829

członkowskim na włączenie innych sektorów czy podsektorów, które uzna za kluczowe lub ważne.

Należy także zwrócić uwagę na art. 2 dyrektywy NIS2, zgodnie z który zakres podmiotowy dyrektywy poza wyjątkami wynikającymi z art. 2 ust.2, obejmie wszystkie przedsiębiorstwa poza małymi i mikroprzedsiębiorstwami. Szczegółowej analizy i wyjaśnienia wymaga sposób określenia w art. 2 ust. 2 kategorii podmiotów, które podlegać będą dyrektywie, nawet jeżeli będą mikro lub małymi przedsiębiorcami. Doprecyzować należy również sposób, w jaki państwa członkowskie będą identyfikować podmioty, o których mowa w art. 2 ust. 2. Za niewystarczający należy uznać termin 6 miesięcy na przesłanie KE listy podmiotów, o których mowa w art. 2 ust. 2 lit. b do f.

4. Już w trakcie dyskusji nad kształtem nowej dyrektywy NIS2, Rząd RP zwracał uwagę na konieczność włączenia administracji publicznej jako jednego z sektorów regulowanych przez dyrektywę. Należy jednak zauważyć, że propozycji przedstawionej przez KE w definicji public administration entity (art. 4 pkt. 23 projektu dyrektywy), pojawia się kryterium dotyczące osobowości prawnej. W przypadku Polski wiele podmiotów administracji publicznej nie posiada ww. osobowości prawnej, co sprawi, że podmioty te nie zostaną objęte regulacjami dyrektywy. Wskazane są zatem aktywne działania rządu RP w celu doprecyzowania definicji. Równocześnie należy jednak pamiętać, że możliwe jest przyjęcie rozwiązań, które mieścić się będą w ramach wynikających z traktatowej podstawy projektu dyrektywy NIS2, a mianowicie art. 114 Traktatu o funkcjonowaniu Unii Europejskiej.

5. Projekt dyrektywy wprowadza podział podmiotów objętych jej zakresem na dwie kategorie podmioty kluczowe (essential) oraz podmioty ważne (important). Projekt wprowadza także jednolite kryterium decydujące o tym, które podmioty są objęte zakresem stosowania dyrektywy. Kryterium to przewiduje stosowanie zasady maksymalnej wielkości (size-cup rule), zgodnie z którą w zakres dyrektywy wchodzą wszystkie średnie i duże przedsiębiorstwa zdefiniowane w zaleceniu KE 2003/361/WE[13], które działają w sektorach objętych zakresem dyrektywy lub świadczą rodzaj usług objęty zakresem niniejszej dyrektywy. Państwa członkowskie nie są zobowiązane do ustanowienia wykazu podmiotów, które spełniają to mające ogólne zastosowanie kryterium związane z wielkością. W konsekwencji każdy średni i duży podmiot z sektora i podsektora, mieszczący się w definicji typu podmiotu wynikającej z załącznika I i II będzie objęty zakresem dyrektywy. Rząd RP zauważa potrzebę doprecyzowania mechanizmu identyfikacji podmiotów kluczowych i ważnych poprzez wprowadzenie dodatkowych kryteriów. Jednym z takich elementów doprecyzowujących może być kwestia wprowadzenia dodatkowych kryteriów wdrażanych na poziomie państwa charakterystycznych dla sektora, podsektora a także konkretnej usługi kluczowej. Rząd RP popiera wyłączenie mikro i małych przedsiębiorstw z zakresu dyrektywy, dostrzegając jednak potrzebę wskazania w dyrektywie wyjątków w tym zakresie. Konieczne jest precyzyjne sformułowanie przepisów dyrektywy. Kwestia identyfikacji podmiotów kluczowych i ważnych generuje wiele pytań i powoduje konieczność dalszej pogłębionej debaty w tym zakresie.

6. Rząd popiera rozwiązania przyjęte w art. 24 projektu odnośnie do jurysdykcji. Jednocześnie Rząd RP wskazuje, że zapisy art. 24 dyrektywy NIS2 wymagają uszczegółowienia w sytuacji,

[13] Zalecenie KE 2003/361/WE z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz. U. WE L 124 z 20.05.2003, s.36)

gdy podmioty jednocześnie świadczą usługi w wielu państwach Unii. Precyzyjne określenie, które państwo w danym przypadku pełni rolę nadzorczą jest kluczowe do zapewnienia prawidłowego funkcjonowania cyberbezpieczeństwa w wymiarze transgranicznym.

7. Rząd RP przychylnie odnosi się do pomysłu utworzenia rejestru, o którym mowa w art. 25 projektu, przy czym w toku negocjacji należy zwrócić uwagę na następujące kwestie. Rząd RP wielokrotnie podkreślał wrażliwość danych, jakimi są informacje o operatorach usług kluczowych, którzy w wielu przypadkach są również wskazani jako operatorzy infrastruktury krytycznej. Dane te nie powinny być publicznie dostępne. W konsekwencji, w toku negocjacji należy dążyć do zapewnienia, że dane z rejestru, o którym mowa w art. 25, nie będą publiczne, jeżeli tak zdecyduje państwo członkowskie. Doprecyzowania przy tym wymaga, w szczególności cel prowadzenia rejestru, zakres danych oraz zasady dostępu do danych.
Należy zauważyć, że zgodnie z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej dyrektywa wyjątkowo może wywoływać skutek bezpośredni wobec przedsiębiorcy albo obywatela, ale tylko wtedy, gdy bezskutecznie minął już termin wdrożenia dyrektywy do krajowego porządku prawnego przez państwo członkowskie, a skutek bezpośredni dotyczy prawa/uprawnienia (a nie obowiązku czy obciążenia), które niewdrożona dyrektywa daje obywatelowi albo przedsiębiorcy. W konsekwencji brzmienie art. 25 wymaga odpowiedniego przeredagowania tak, aby obowiązki nie były nałożone bezpośrednio na podmioty kluczowe i ważne.

8. Współpraca pomiędzy państwami członkowskimi w przypadku incydentów dużej skali jest jednym z kluczowych aspektów wzmocnienia cyberbezpieczeństwa całej Unii. Z tego względu inicjatywę powołania CyCLONe należy ocenić pozytywnie. Mechanizm ten nie powinien jednak powielać już istniejących kanałów współpracy, takich jak chociażby Sieć CSIRT, poprzez którą na poziomie operacyjnym współpracują ze sobą krajowe CSIRTy. Obecny zapis artykułu 14 dyrektywy NIS2 jest bardzo ogólny, nie precyzujący miejsca tej sieci w europejskim systemie cyberbezpieczeństwa. Zwrócić należy uwagę, że zgodnie z obecnymi założeniami CyCLONe nie będzie miał kompetencji operacyjnych, a także nie będzie miał oddzielnego kanału zbierania informacji o incydentach, lecz będzie bazował na tych otrzymywanych np. z CSIRT poziomu krajowego, zatem będzie jedynie przekazywał te same informacje co Sieć CSIRT, czy Grupa Współpracy NIS. Należy zatem doprecyzować przepisy w tym zakresie, tak aby w istocie wprowadzenie przepisów dotyczących CYCLONe miało wartość dodaną poprzez wzmocnienie koordynacji i współpracy w przypadku wystąpienia incydentów dużej skali.

Rząd RP pozytywnie ocenia wprowadzenie regulacji w zakresie cyberbezpieczeństwa infrastruktury krytycznej. Mając na uwadze, że wiele (a nawet większość) podmiotów będących operatorami usług kluczowych jest również operatorami infrastruktury krytycznej, pomysł ustanowienia ram zarządzania kryzysowego w cyberbezpieczeństwie i jego koordynacji wydaje się zmierzać w dobrym kierunku. Niemniej jednak ważne jest zapewnienie spójności rozwiązań przyjętych w NIS2 a dyrektywą Parlamentu Europejskiego i Rady UE w sprawie odporności podmiotów krytycznych COM/2020/829, oraz nie duplikowanie struktur koordynacyjnych przewidzianych w tych aktach. Rząd RP uważa, że wprowadzenie przepisów związanych z Zaleceniem w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę (tzw. Blueprint) w celu osiągnięcia możliwie najlepszych synergii między mechanizmami zarządzania kryzysowego na poziomie UE (i państw członkowskich) a przepisami dotyczącymi cyberbezpieczeństwa to dobry pomysł. Rząd RP pozytywnie odnosi

się do propozycji opracowania przez każde państwo członkowskie ram zarządzania kryzysowego w obszarze cyberbezpieczeństwa (plany, o których mowa w art. 7 ust. 3). W sytuacji gdy państwa członkowskie uwzględniają zagadnienia wymagane w tych planach, w ramach szerszej dokumentacji dotyczącej zarządzania kryzysowego, należy zapewnić, że nie będzie konieczności ustanawiania oddzielnych planów w tym zakresie.

9. W ocenie Rządu RP harmonizacja kar dotyczących nie wykonania obowiązków nałożonych na podmioty objęte regulacjami jest właściwym kierunkiem. Jednakże, Rząd RP w toku negocjacji będzie dążył do wyjaśnienia zasadności i konieczności przyjęcia kar w zaproponowanej wysokości wskazując, że są one wysokie oraz podkreślając konieczność adekwatności, proporcjonalności i spełnienia przez nie roli odstraszającej. Z obserwacji organów właściwych we współpracy z podmiotami regulowanymi, otwarte podejście, w tym wymiana informacji oraz budowanie zaufania z podmiotami regulowanymi odnosiły znacznie lepsze efekty niż groźba nałożenia kar. Zbyt duża wysokość kar może wpłynąć negatywnie na współpracę pomiędzy organami właściwymi a podmiotami regulowanymi. W kontekście rozbudowanych funkcji nadzorczych organów właściwych ds. cyberbezpieczeństwa oraz wysokich kar finansowych przewidzianych w zapisach dyrektywy, kluczowe jest uwzględnienie w projekcie zapisów rozdzielających funkcje nadzorcze od funkcji CSIRT. W związku z powyższym Rząd RP będzie postulował, by zapisy w dyrektywie w zakresie kar, nie spowodowały „usztywnienia" relacji na linii organ właściwy/CSIRT a podmiot regulowany, gdyż może to w rezultacie zmniejszyć cyberbezpieczeństwo kraju zamiast je wzmacniać.

10. W kontekście propozycji prowadzenia przez ENISA rejestru podatności (art. 6 propozycji) Rząd RP stoi na stanowisku, że jest to pozytywna zmiana. Jednakże, przepisy dyrektywy NIS2 wymagają doprecyzowania. Wyjaśnienia wymaga, w szczególności jakiego rodzaju podatności mają być rejestrowane, jakie będą warunki dostępu do rejestru, czy będzie to rejestr publiczny. Uściślenia wymagają także zapisy związane z koordynującą rolą CSIRT w zakresie ujawniania podatności, na czym ma polegać taka rola, jakie podatności mają podlegać zgłaszaniu, w jaki sposób je ujawniać. Wyjaśnienia wymaga także, czy przed przekazaniem informacji do rejestru wyznaczony CSIRT będzie weryfikować zgłoszenie, a także zdolności techniczne i organizacyjne ENISA do realizacji tego zadania, w tym analizy zgłoszonych podatności pod kątem ich faktycznego występowania. Powstaje też wątpliwość, czy operatorzy kluczowi i ważni będą posiadali wszelkie niezbędne informacje w przypadku gdy będą korzystać z oprogramowania zewnętrznego.

11. Rząd RP w toku przeglądu dyrektywy NIS zwrócił uwagę na problem regulacji w zakresie łańcucha dostaw, przede wszystkim w kontekście sieci 5G. Należy podkreślić, że realizacja tego zadania wymaga przeprowadzenia stosownych analiz, np. zależności pomiędzy sektorami oraz inwentaryzacji dostawców. Pociąga to za sobą konieczność stworzenia właściwych narzędzi i zbudowanie kompetencji w organach właściwych lub CSIRTach. Dlatego konieczne będzie zapewnienie odpowiedniego finansowania w tym zakresie. Dodatkowo, na poziomie UE powinna powstać wspólna metodyka związana z cyberbezpieczeństwem łańcucha dostaw. W realizację tego zadania powinna być zaangażowana ENISA, sieć CSIRT oraz Grupa Współpracy. Wskazane byłoby, aby zapisy na temat wytworzenia takiej metodyki znalazły się w dyrektywie.

12. Rząd RP z zadowoleniem przyjmuje propozycję KE dotyczącą zmian w regulacji i nadzorze nad dostawcami usług cyfrowych. Sektor ten jest jednym z kluczowych w dobie cyfryzacji

usług, gdyż, jak wskazują analizy, wielu operatorów usług kluczowych przy świadczeniu swoich usług wykorzystuje systemy i usługi świadczone przez tych dostawców.

13. Ocena i skuteczność funkcjonowania wdrożonych regulacji z poziomu unijnego jest bardzo istotną rzeczą. Wprowadzenie mechanizmu „peer rewiew" wymaga jednak szczegółowej analizy i dyskusji w kontekście zapewnienia przejrzystości tego mechanizmu, jego dobrowolności oraz wartości dodanej jego wprowadzenia. Mechanizm „peer review" powinien być dobrowolny. W ocenie Rządu RP należy położyć nacisk na przedsięwzięcia związane z budowaniem zdolności państw członkowskich w obszarze cyberbezpieczeństwa, gdyż jest to bardziej efektywne niż wyłącznie analiza poprawności wdrożenia przepisów NIS.

14. Rząd RP popiera wzmocnienie kompetencji organów właściwych oraz rozszerzenie zadań CSIRT. Zapewnienie cyberbezpieczeństwa wymaga odpowiednich uprawnień organów właściwych. Propozycje zawarte w art. 10 i 29 projektu w ocenie Rządu RP zapewniają realizację tego celu.

15. Jednym z kluczowych działań w zakresie analizowania incydentów poważnych i istotnych jest ich raportowanie przez państwa członkowskie, a następnie dokonanie ich analizy w celu wyciągnięcia wniosków dotyczących cyberbezpieczeństwa całej UE. Rząd RP wielokrotnie zwracał uwagę na spore rozbieżności pomiędzy krajami w tym zakresie. Dlatego też koniecznym jest ustalenie minimalnych kategorii incydentów, w celu uwspólniania raportowania pośród państw członkowskich. W innym wypadku zbiorcze dane od wszystkich krajów UE nie pozwolą na dogłębną analizę incydentów cyberbezpieczeństwa Unii.

W związku z powyższym, Rząd RP uważa za konieczne dokonanie przeglądu zarówno sposobu raportowania, jak i nowych propozycji wymiany informacji pomiędzy organami właściwymi, CSIRTami a organami właściwymi w ramach np. infrastruktury krytycznej, w celu ustalenia wspólnego horyzontalnego podejścia akceptowalnego przez wszystkie państwa członkowskie, co do sposobu i zakresu wymiany informacji w zakresie incydentów oraz ich raportowania do KE. Korzystnym rozwiązaniem mogą być akty implementacyjne KE, o których mowa w art. 20 ust. 11 projektu, przy czym wprowadzenie tej instytucji wymaga szczegółowej analizy.

16. Zapewnienie kompletnego i dostępnego rejestru domen najwyższego poziomu (TLD) stanowi istotny element wzmocnienia cyberbezpieczeństwa. Stąd też ujednolicenie zapisów na poziomie europejskim wydaje się właściwym kierunkiem.

17. Rząd RP pozytywnie odnosi się do propozycji dotyczących wykorzystania certyfikacji i standaryzacji w obszarze cyberbezpieczeństwa. Wymogi dotyczące certyfikacji niektórych produktów, usług i procesów ICT mogą stanowić instrument wykazania zgodności z wymogami określonymi w dyrektywie. Podkreślenia przy tym wymaga, że wszelkie rozwiązania dotyczące certyfikacji muszą być zgodne z Aktem o Cyberbezpieczeństwie, a zakres wykorzystania certyfikacji wymaga szczegółowej analizy.

18. Rząd RP przychylnie odnosi się do propozycji dotyczącej porozumień w zakresie dzielenia się informacjami w obszarze cyberbezpieczeństwa (art. 26 projektu), przy czym propozycja ta wymaga szczegółowego wyjaśnienia i doprecyzowania.

19. Rząd RP popiera włączenie w ramy ustanowione w NIS zgłaszania incydentów na podstawie rozporządzenia 910/2014 (e-IDAS) oraz dyrektywy 2018/1972 (EKŁE), przy czym pogłębionej analizy wymaga zakres zmian koniecznych w tych aktach dla zapewnienia spójności przyjętych rozwiązań w szczególności w zakresie nadzoru.

Ocena skutków prawnych

Zgodnie z art. 288 Traktatu o Funkcjonowaniu Unii Europejskiej, dyrektywa jako forma aktu prawnego wiąże każde Państwo Członkowskie, do którego jest kierowana, w odniesieniu do rezultatu, który ma być osiągnięty, pozostawia jednak organom krajowym swobodę wyboru formy i środków. Przepisy dyrektywy powinny być więc implementowane do polskiego systemu prawnego za pomocą krajowych aktów prawnych. Wdrożenie dyrektywy w polskich warunkach będzie w szczególności wymagało nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560 z późn. zm.) oraz aktów wykonawczych, ale również ustawy - Prawo telekomunikacyjne (t.j. Dz.U. z 2019 r. poz. 2460 z późn. zm.), ustawy o zarządzaniu kryzysowym (t.j. Dz.U. z 2020 r. poz. 1856 z późn. zm.), ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz.U. z 2020 r. poz. 1173 z późn. zm.).

Ocena skutków społecznych

Zgodnie z oceną potencjalnego wpływu regulacji na społeczeństwo, wprowadzenie projektu ma poprawić poziom odporności cyfrowej w Unii Europejskiej. W zależności od ostatecznego kształtu proponowanej dyrektywy, istnieje kilka wariantów oceny skutków społecznych. Jeden z nich, bardziej ograniczony, dotyczący rozbudowy już istniejących środków, zakłada poprawienie poziomu ochrony przeciw negatywnym skutkom incydentów cyberbezpieczeństwa, co można ocenić jako niewielki, jakkolwiek pozytywny skutek społeczny. Druga opcja zakłada wprowadzenie zarządzania kryzysowego i nadzór nad zgodnością pomiędzy podmiotami publicznymi i prywatnymi w zakresie cyberbezpieczeństwa. Nowe środki, zakładane w tej opcji, pozwoliłyby na zapewnienie zwiększonego poziomu cyberbezpieczeństwa dla obywateli, zwiększonego zaufania do firm i infrastruktury teleinformatycznej oraz wysokiego poziomu cyberbezpieczeństwa i zdolności do radzenia sobie z incydentami cyberbezpieczeństwa i do przeciwdziałania im. Dodatkowo, wprowadzenie podejścia operacyjnego może przyczynić się do pozytywnych skutków społecznych w innych obszarach, np. poprzez zmniejszenie poziomu cyberprzestępstw i zwiększony poziom ochrony przeciw incydentom cyberbezpieczeństwa i naruszeniom ochrony danych.

Ocena skutków gospodarczych

Głównym kosztem dla przedsiębiorstw wynikającym z dyrektywy NIS są koszty przystosowania się do nowych przepisów tj. wprowadzenia wymogów bezpieczeństwa, obowiązku zgłaszania incydentów i zastosowania środków nadzorczych. Zwiększenie kosztów tych działań potencjalnie pozwoli jednak na uniknięcie kosztów spowodowanych incydentami cyberbezpieczeństwa.

Ocena skutków finansowych

Szacowane korzyści proponowanej zmiany dyrektywy NIS, oparte na modelowaniu ekonomicznym opracowanym przy badaniu w ramach przeglądu bezpieczeństwa sieci i informacji wskazują, że preferowane rozwiązanie może prowadzić do obniżenia kosztów incydentów cyberbezpieczeństwa o 11,3 mld EUR w ciągu dziesięciu lat. Ten kierunek zmian skutkuje kosztami dla organów państw członkowskich, związanych ze stosowaniem nowego prawa. Szacuje się, że nowe zadania, które nakłada projekt NIS2 będą wymagały zwiększenia zasobów (w tym personelu) właściwego organu krajowego o 20-40%. Według szacunków, wzrost ten będzie związany z potrzebą prowadzenia nadzoru nad większą ilością podmiotów (np. kontrola, audyt czy ocena zgodności) i zwiększoną interakcją z przedsiębiorcami. W przypadku przedsiębiorstw podpadających pod zakres NIS2, szacuje się, że w pierwszych latach po wprowadzeniu nowych ram bezpieczeństwa sieci i informacji, przedsiębiorstwa te zwiększą maksymalnie wzrost swoich obecnych wydatków na bezpieczeństwo ICT o 22 % (byłoby to 12 % w przypadku przedsiębiorstw już objętych zakresem obecnej dyrektywy w sprawie bezpieczeństwa sieci i informacji). Implementacja dyrektywy NIS2 do polskiego porządku prawnego będzie skutkowała podniesieniem wydatków z budżetu państwa na wzmocnienie kadr m.in. w organach właściwych oraz zespołach CSIRT poziomu krajowego, co będzie wiązać się ze zwiększeniem wydatków z budżetu państwa.

Rząd RP będzie dążył do tego, aby ewentualne koszty, przede wszystkim osobowe, zostały sfinansowane w ramach limitu wydatków, określonych w ustawie budżetowej na dany rok we właściwych częściach budżetowych. Jednak biorąc pod uwagę konieczność wyznaczenia dodatkowych organów właściwych, w związku z określeniem nowych sektorów ważnych i kluczowych (załączniki I i II w projekcie dyrektywy NIS2), m.in. zaopatrzenie w żywność oraz usługi pocztowe kurierskie, których nie przewiduje obecna ustawa o krajowym systemie cyberbezpieczeństwa, pojawi się potrzeba zapewnienia finansowania nowych organów właściwych. Ponadto stale rosnąca liczba cyberataków i incydentów, których skutkują w przerwach w świadczeniu usług kluczowych np. w sektorze zdrowia (cyberataki na szpitale), wyraźnie wskazują na stale rosnącą presję do wzmocnienia cyberbezpieczeństwa RP, zatem Rząd RP nie może wykluczyć, że na etapie implementacji Dyrektywy NIS2 pojawi się potrzeba wyasygnowania dodatkowych środków z budżetu państwa. Wszelkie wydatki potrzebne na realizację zadań, o których mowa w zmienianej dyrektywie NIS, będą sfinansowane w ramach limitu wydatków odpowiednich dysponentów części budżetowych.

Jednocześnie Rząd RP będzie dążył do podejmowania działań mających na celu ograniczenie ewentualnych skutków obciążających kraje członkowskie pod kątem finansowym.

Stanowiska Partnerów Społecznych:

Mając na uwadze społeczny i gospodarczy wymiar skutków wdrożenia projektu zmian w dyrektywie w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Kancelaria Prezesa Rady Ministrów, w ramach prac nad projektem stanowiska rządu, zwróciła się do licznych partnerów społecznych z prośbą o odniesienie się do przygotowanego dokumentu.

5 stycznia br. zostało przekazane formalne zaproszenie do wzięcia udziału w konsultacjach do 6 ministerstw i urzędów współpracujących oraz 3 zespołów CSIRT poziomu krajowego.

Jednocześnie zaproszenie zostało przekazana do ponad 80 partnerów społecznych – izb, fundacji oraz stowarzyszeń branżowych oraz 90 firm. Kancelaria Prezesa Rady Ministrów zbierała uwagi do 26 stycznia br.

Uwagi zostały zgłoszone przez: dwie osoby prywatne, Fundację Bezpieczna Cyberprzestrzeń, Polską Izbę Radiodyfuzji Cyfrowej, Polski Związek Przemysłu Motoryzacyjnego, Polską Izbę Informatyki i Telekomunikacji, Stowarzyszenie ISACA Warszawa, Międzynarodowe Centrum Bezpieczeństwa Chemicznego (ICCSS) w Warszawie, Konfederację Lewiatan, Intelligent Logistic Solutions Sp. z o.o.

Polska Izba Radiodyfuzji Cyfrowej, Polska Izba Informatyki i Telekomunikacji oraz Konfederacja Lewiatan postulują:

1. usunięcie przedsiębiorców telekomunikacyjnych z listy podmiotów objętych zakresem zastosowania projektowanej dyrektywy NIS2 i pozostawienie w mocy przepisów Europejskiego Kodeksu Łączności Elektronicznej dotyczących bezpieczeństwa sieci i usług telekomunikacyjnych;
2. usunięcie z projektowanej dyrektywy przepisów upoważniających Komisję Europejską do określania zakresu obowiązków w zakresie cyberbezpieczeństwa mocą aktów delegowanych;
3. wstrzymanie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa do momentu ustalenia ostatecznego kształtu dyrektywy NIS;
4. zapewnienie zgodności przepisów projektowanej dyrektywy w zakresie certyfikacji z Aktem o cyberbezpieczeństwie;
5. zracjonalizowanie, przez dziesięciokrotne obniżenie, maksymalnego wymiaru kar, które mogą być nakładane za naruszenie wymogów w zakresie cyberbezpieczeństwa oraz zapewnienie, że wymiar kary, która może być nałożona za dane naruszenie, jest taki sam bez względu na to, czy podmiot dopuszczający się naruszenia jest przedsiębiorcą prywatnym czy podmiotem administracji publicznej;
6. zmianę definicji podmiotu administracji publicznej, tak, aby definicja ta w polskich warunkach faktycznie obejmowała podmioty administracji publicznej;
7. usunięcie przepisu dyrektywy nakładającego bezpośrednio na przedsiębiorców obowiązek zgłoszenia do ENISA oraz zapewnienie, że prowadzone na szczeblu unijnym lub krajowym wykazy lub rejestry będą jawne i publicznie dostępne.
8. wprowadzenie dodatkowych kryteriów dla kwalifikacji podmiotów jako kluczowych lub istotnych, w celu zapewnienia większej proporcjonalności wprowadzonych przepisów oraz ograniczenia nadmiarowych obciążeń nakładanych na przedsiębiorców;
9. doprecyzowanie przepisów w zakresie raportowania incydentów i zagrożeń;
10. zharmonizowanie i ujednolicenie definicji we wszystkich aktach prawnych dotyczących rynku cyfrowego;
11. doprecyzowanie przepisów dot. współpracy w zakresie cyberbezpieczeństwa;
12. ograniczenie zakresu stosowania dyrektywy NIS do wszystkich podmiotów wyszczególnionych w załącznikach, w szczególności poprzez ocenę skutków potencjalnych incydentów u tych grup podmiotów i wprowadzenie na tej podstawie precyzyjnych kryteriów klasyfikacji;
13. jednoznaczne określenie obowiązków w zakresie raportowania;

14. wskazanie, że obowiązkiem certyfikacji objęty może być producent albo inny podmiot wprowadzający produkt na rynek, bez obejmowania obowiązkiem certyfikacji obszaru kompetencji oraz rezygnacji z obowiązków certyfikacyjnych;
15. wprowadzenie pojedynczego punktu nadzoru nad podmiotami świadczącymi usługi transgraniczne;
16. harmonizacja rejestracji podmiotów objętych regulacją dyrektywy;
17. rezygnacja z udziału notyfikacji wymiany informacji;
18. rezygnacja z publicznego piętnowania braku zgodności;
19. doprecyzowanie przepisów związanych z regulacją łańcucha dostaw;

Fundacja Bezpieczna Cyberprzestrzeń. W motywie 54 poruszona została kwestia szyfrowania end-to-end. Szyfrowanie o jakim mówi dyrektywa, takim szyfrowaniem nie jest, ponieważ szyfrowanie end-to-end wyklucza dostęp stron trzecich do zabezpieczonej komunikacji. Udzielenie dostępu do zaszyfrowanej informacji stronie trzeciej sprawia, że przestaje ona być informacją zaszyfrowaną.
Fundacja zwraca uwagę na obowiązek dotyczący zgłaszania incydentu poważnego w ciągu 24 godzin. W jej ocenie termin 24 godzinny powinien być nieprzekraczalny w żadnym wypadku, 24 godziny to czas wystarczający na przygotowanie wstępnego zgłoszenia, które ma zawierać wyłącznie informacje absolutnie niezbędne do poinformowania właściwych organów o samym zdarzeniu.
Fundacja zwraca także uwagę na kwestie definicji zawarte w dyrektywie, które powinny zostać zweryfikowane.

Osoba fizyczna nr 1 zwraca uwagę, że dokument jest na zbyt dużym poziomie ogólności.

Polski Związek Przemysłu Motoryzacyjnego (PZPM) wskazuje, że dyrektywa wydaje się nakładać na branżę dodatkowe obciążenie obok regulaminu UNECE R155 w sprawie cyberbezpieczeństwa i zbliżającego się aktu wykonawczego UE w sprawie cyberbezpieczeństwa opartego na rozporządzeniu 2019/2144 (GSR). Dlatego też PZPM obawia się, że proponowany Aneks 2 w przypadku branży motoryzacyjnej będzie stanowił nad regulację wobec obecnie toczących się prac nad aktami sektorowymi w tym obszarze.

Stowarzyszenie ISACA Warszawa. W opinii Stowarzyszenia zapisy zaproponowane w dyrektywie NIS2 (artykuły:16, 19, 21) pozbawiają podmioty krajowe, które są odpowiedzialne za implementację dyrektywy, realnego wpływu na to, jak kształtowane są rozwiązania cyberbezpieczeństwa na terenie danego kraju członkowskiego.
Jednocześnie Stowarzyszenie uważa, że stworzenie rejestru podatności prowadzonego przez ENISA jest ważne. Należy zagwarantować podmiotom europejskim bezpłatny dostęp do takiego rejestru oraz możliwość bezpłatnego korzystania z narzędzi (jeśli takowe będą) wypracowanych przez ENISA w celu zwiększenia odporności na cyberataki.
Wg Stowarzyszenia proponowane wysokości kar w korelacji z wymaganiami narzuconymi przez artykuły 19 i 21 mogą prowadzić do eliminacji pewnych podmiotów gospodarczych.

Międzynarodowe Centrum Bezpieczeństwa Chemicznego (ICCSS) w Warszawie proponuje:
powołanie w ramach dyrektywy NIS 2 grupy pt.: Industrial Reliability and Cybesecurity Group;
wdrożenie kwalifikacji w cyberbezpieczeństwie dla osób, które projektują/integrują, wykonują oraz eksploatują produkty, usługi, procesy w ramach CSA, a także wykonują i nadzorują

badania certyfikacyjne dla produktów, usług, procesów. System taki został wdrożony w Polsce w końcu 2020 przez opublikowanie 3 kompetencji rynkowych. System wdrożony w Polsce może być przykładem dla UE.

Osoba fizyczna nr. 2 proponuje: Oprócz rejestru podatności, o którym mowa w art. 6 ust. 2 proponowanej dyrektywy, Unia Europejska powinna aktywnie wspierać oraz usuwać przeszkody w badaniu i identyfikowaniu podatności w produktach i usługach ICT.

Intelligent Logistic Solutions Sp. z o.o. proponuje:

- aby dla dostawców usług w chmurze lub usług przetwarzania danych jako wytyczne wprowadzić normy ISO 27701, ISO 27017 oraz ISO 27018 – jako zalecenie lub wymaganie - (Motyw 18),
- rozszerzenie zakresu z cyberincydentu na incydent (szeroko pojęty), aby dla potrzeb szacowania ryzyka było więcej wziętych pod uwagę obszarów - Motyw 38,
- zwiększyć częstotliwość oceny krajowych strategii cyberbezpieczeństwa, aby co 2 lub 3 lata odbywał się przegląd. Czteroletnie okresy w perspektywie cyberbezpieczeńtwa to bardzo odległy okres - (Rozdział II, art. 5 pkt 4),
- doprecyzowanie „bezpiecznego miejsca", gdyż tego typu stwierdzenie może prowadzić do nadinterpretacji lub niejasności ze strony wykonawców ustawy i/lub dyrektywy (Rozdział II, art. 10 pkt 1b).

Wnioski

1. Nowa dyrektywa NIS2 jest oczekiwaną i potrzebną regulacją w obszarze cyberbezpieczeństwa.
2. Jako regulacja horyzontalna swoim działaniem dyrektywa obejmie szeroki zakres sektorów oraz działających w nich podmiotów, dzięki czemu zostanie zwiększone cyberbezpieczeństwo zarówno na poziomie krajowym, jak i całej UE.
3. Nowa dyrektywa adresuje wiele niedociągnięć, na które zwracał uwagę Rząd Polski w trakcie implementacji dyrektywy NIS w poprzednich latach. Wprowadzone zmiany w znacznym stopniu zniwelują problemy związane z kwestiami dotyczącymi jurysdykcji, dostawców usług cyfrowych, kwestii raportowania incydentów, łańcucha dostaw oraz wielu innych.
4. Nowa dyrektywa znacznie wzmocni także kwestie związane ze współpracą pomiędzy poszczególnymi państwami członkowskimi Unii, dając im narzędzia do wymiany informacji i koordynacji działań w obszarze politycznym, strategicznym oraz operacyjnym.
5. Jako część pakietu cyberbezpieczeństwa Unii Europejskiej nowelizacja dyrektywy NIS wraz ze Strategią UE w zakresie cyberbezpieczeństwa na cyfrową dekadę, pozwoli na znaczne wzmocnienie Unii na arenie międzynarodowej w kontekście bezpieczeństwa.

IV. Informacja w sprawie zgodności projektu aktu z zasadą pomocniczości

Wniosek jest zgodny z zasadą pomocniczości.

V. Przedstawiciel Rządu upoważniony do prezentowania stanowiska

Pan Marek Zagórski, Sekretarz Stanu w Kancelarii Prezesa Rady Ministrów, Pełnomocnik Rządu ds. Cyberbezpieczeństwa