Nazwa projektu Ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Paweł Olszewski Sekretarz Stanu w Ministerstwie Cyfryzacji **Kontakt do opiekuna merytorycznego projektu** Łukasz Wojewoda, Dyrektor Marcin Wysocki, Zastępca Dyrektora Departament Cyberbezpieczeństwa Ministerstwa Cyfryzacji email: Sekretariat.DC@cyfra.gov.pl tel. + 48 22 245 59 22	**Data sporządzenia** 03.10.2024 **Źródło:** Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80). Rozporządzenie delegowane Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 Kamień milowy reformy C3.1. Krajowego Planu Odbudowy i Zwiększania Odporności Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo **Nr w wykazie prac** UC32

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Projektowana ustawa ma na celu wdrożenie dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022 str. 80), zwanej dalej „dyrektywą NIS 2".

Pojawianie się nowych cyberzagrożeń, jak również szybki wzrost katalogu usług publicznych dostępnych online powodują, że instytucje publiczne jak i podmioty prywatne odpowiedzialne za cyberbezpieczeństwo będą zmuszone poświęcać coraz więcej środków na zapewnienie cyberbezpieczeństwa. Zmieniająca się sytuacja międzynarodowa oraz konieczność dostarczenia usług dużej grupie nowych klientów sprawia, że niezbędne jest dalsze wzmacnianie podmiotów krajowego systemu cyberbezpieczeństwa. Tą sytuację uwidaczniają statystyki zespołu CSIRT NASK. W 2022 r. do zespołu CSIRT NASK zgłoszono ponad 39 000 incydentów cyberbezpieczeństwa, a w 2023 r. ponad 75 000 incydentów cyberbezpieczeństwa. Dyrektywa NIS 2 i przepisy ją implementujące są odpowiedzią na dynamicznie zmieniającą się sytuację w cyberprzestrzeni.

Dyrektywa NIS 2 zastąpiła dotychczasowy podział na operatorów usług kluczowych i dostawców usług cyfrowych określony w dyrektywie 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 (Dz. Urz. UE L 194 z 19.07.2016, str. 1), zwanej dalej „dyrektywą NIS 1", na podmioty kluczowe i podmioty ważne. Ponadto rozszerzeniu uległ katalog sektorów objętych dyrektywą. Dyrektywa NIS 2 nakłada również szereg obowiązków na podmioty kluczowe i podmioty ważne. Jako podstawowy obowiązek należy wskazać stosowanie odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu.

Zauważono również, że uprawnienia Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa są niewystarczające w stosunku do zadań, które organ ten musi wypełniać. Pełnomocnikowi Rządu do Spraw Cyberbezpieczeństwa brakuje skutecznych środków oddziaływania na podmioty krajowego systemu cyberbezpieczeństwa. W przeciwieństwie do innych Pełnomocników Rządu nie ma on uprawnień do żądania niezbędnych informacji od organów administracji rządowej, możliwości powoływania zespołów problemowych, czy zlecania badań. Pełnomocnikowi Rządu do Spraw Cyberbezpieczeństwa brakuje również środka prawnego, który umożliwiłby wydawanie rekomendacji o charakterze technicznym (w tym zakresie – Narodowych Standardów Cyberbezpieczeństwa, o których mowa w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, zwaną dalej :Strategią") i jednocześnie obowiązku uwzględnienia tych rekomendacji przez podmioty krajowego systemu cyberbezpieczeństwa, w trakcie procesu zarządzania ryzykiem.

Do tej pory zostały utworzone tylko dwa sektorowe zespoły cyberbezpieczeństwa – CSIRT KNF i CSIRT Centrum e-Zdrowie. W pozostałych sektorach gospodarki brakuje zespołów wspierających przedsiębiorców w reagowaniu na incydenty. Utworzenie tych zespołów przewiduje Inwestycja C3.1.1 Krajowego Planu Odbudowy i Zwiększania Odporności, zwanego dalej „KPO", *Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo*. Planowana jest realizacja projektu pod nazwą „utworzenie lub rozwój przynajmniej 5 sektorowych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT)".

Komisja Europejska wielokrotnie, m.in. w opublikowanych w marcu 2019 r. zaleceniach dot. cyberbezpieczeństwa sieci 5G podkreślała, że kwestia zapewnienia bezpieczeństwa wdrażanej technologii 5G jest priorytetem. Potwierdzenie tego znajduje swój wymiar w opublikowanym w styczniu 2020 r. zestawie środków dot. minimalnej harmonizacji i standaryzacji na poziomie Unii Europejskiej rozwiązań cyberbezpieczeństwa sieci 5G, określanego jako 5G Toolbox[1)]. Zestaw obejmuje zarówno narzędzia o charakterze strategicznym i technicznym, jak i te o charakterze wspierającym. Cele są dwa: po pierwsze bezpieczeństwo sieci 5G, po drugie uspójnienie polityk państw członkowskich w obszarze bezpieczeństwa technologii 5G. 5G Toolbox zawiera także definicje zestawu środków zabezpieczających na poziomie strategicznym i technicznym oraz wskazuje działania wspierające stosowanie tych środków dla ograniczenia ryzyk cyberbezpieczeństwa w sieciach 5G, które będą kręgosłupem Jednolitego Rynku Cyfrowego (JRC) UE. Wyróżnione są m.in. środki o charakterze:

1) strategicznym – m.in. większe uprawnienia dla organów właściwych, w tym ocena ryzyka dostawców sprzętu lub oprogramowania (środek strategiczny SM03);
2) technicznym – m.in. badanie bezpieczeństwa oprogramowania i urządzeń – uprawnienia Pełnomocnika Rządu ds. Cyberbezpieczeństwa oraz zespołów CSIRT poziomu krajowego: CSIRT MON, CSIRT NASK, CSIRT GOV – wynikające z art. 33 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222), zwanej dalej „KSC";
3) wspierającym – m.in. dotyczące prac nad europejskim programem standaryzacji i certyfikacji cyberbezpieczeństwa.

Obecnie brakuje także podstawy prawnej do przeprowadzenia identyfikacji dostawców sprzętu lub oprogramowania, którzy stwarzają zagrożenie dla bezpieczeństwa narodowego, tym samym nie jest wdrożony środek SM03 z Toolboxa 5G.

Podsumowując aby wdrożyć dyrektywę NIS 2 oraz postanowienia Toolboxa 5G konieczne jest wprowadzenie zmian na poziomie ustawowym.

Aby zapewnić stosowanie rozporządzenia delegowanego Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci

[1)] *Cybersecurity of 5G networks. EU Toolbox of risk mitigating measures,* https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej należy wyznaczyć organ, który będzie realizował zadania nadzorcze wynikające z tego rozporządzenia.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Zmiany wprowadzone przez dyrektywę NIS 2 oraz pojawiające się nowe cyberzagrożenia powodują konieczność wprowadzenia stosownych zmian w KSC. Jest to podstawowy akt dotyczący cyberbezpieczeństwa w Polsce, który poprzednio wdrożył dyrektywę NIS 1. Istotne jest uspójnienie krajowego systemu cyberbezpieczeństwa z rozwiązaniami europejskimi. Poprzez zmianę KSC wdrożone zostaną także postanowienia Toolboxa 5G.

Nowelizacja KSC polega w szczególności na:

1) rozszerzeniu katalogu podmiotów krajowego systemu cyberbezpieczeństwa o nowe sektory gospodarki (ścieki, zarządzanie ICT, przestrzeń kosmiczna, poczta, produkcja, produkcja i dystrybucja chemikaliów, produkcja i dystrybucja żywności);
2) nałożeniu obowiązków z zakresu środków zarządzania ryzykiem na podmioty kluczowe i podmioty ważne w cyberbezpieczeństwie, dotyczące w szczególności stosowania odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych, zgodne z dyrektywą NIS 2;
3) wprowadzeniu odpowiedzialności kierownika podmiotu kluczowego lub podmiotu ważnego za realizację zadań z zakresu cyberbezpieczeństwa – kierownik takiego podmiotu będzie odpowiedzialny za realizację tych zadań przez dany podmiot; w przypadku niewywiązania się z tych zadań na kierownika będą mogły być nałożone kary; kierownik będzie obowiązany również do przejścia stosownego szkolenia z zakresu cyberbezpieczeństwa;
4) wprowadzeniu możliwości zgłaszania incydentów przez podmioty kluczowe i podmioty ważne, za pomocą systemu teleinformatycznego ministra właściwego do spraw informatyzacji, zwanego dalej „ministrem", do właściwych zespołów CSIRT sektorowych i CSIRT poziomu krajowego;
5) utworzeniu zespołów CSIRT sektorowych w poszczególnych sektorach gospodarki, które będą wspierać podmioty kluczowe i podmioty ważne w obsłudze incydentów cyberbezpieczeństwa;
6) wzmocnieniu kompetencji nadzorczych organów właściwych do spraw cyberbezpieczeństwa, polegających na możliwości wydawania ostrzeżeń, wyznaczania urzędnika monitorującego wykonywanie obowiązków przez dany podmiot kluczowy albo podmiot ważny, nakazywanie przeprowadzenia oceny bezpieczeństwa systemu informacyjnego, nakazywanie przeprowadzenia audytu bezpieczeństwa;
7) wprowadzeniu nowych kar pieniężnych za niewykonanie obowiązków ustawowych przez podmioty kluczowe i podmioty ważne, m. in. za nie wdrożenie systemu zarządzania bezpieczeństwem informacji czy nie zarejestrowanie się w wykazie podmiotów kluczowych i podmiotów ważnych;
8) wprowadzeniu Krajowego Planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę;
9) rozszerzeniu kompetencji ministra (organ ten będzie mógł dokonać, w drodze decyzji, prawnej identyfikacji dostawcy wysokiego ryzyka, będzie mógł też wydać polecenie zabezpieczające ze wskazaniem zachowania, które ograniczy skutki trwającego incydentu krytycznego);
10) wzmocnieniu pozycji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa poprzez wyposażenie go w konkretne uprawnienia w zakresie wydawania rekomendacji mających na celu wzmocnienie poziomu cyberbezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa; Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa będzie mógł także żądać informacji niezbędnych do wykonywania jego zadań od organów administracji rządowej oraz zlecać wykonanie badań niezbędnych do realizacji jego zadań; Pełnomocnikowi Rządu do Spraw Cyberbezpieczeństwa umożliwi się także zakupy oprogramowania z zakresu cyberbezpieczeństwa dla podmiotów publicznych;
11) rozszerzeniu kompetencji zespołów CSIRT poziomu krajowego, w tym CSIRT NASK, co jest związane ze zwiększoną liczbą podmiotów kluczowych i ważnych, którym CSIRT NASK będzie udzielał wsparcia w reagowaniu na incydenty;
12) rozwijaniu kompetencji ministra w zakresie edukacji cyberbezpieczeństwa – przewiduje się środki na prowadzenie kampanii edukacyjnych i programów z zakresu cyberbezpieczeństwa.

Projekt ustawy służy również realizacji celów Strategii, jakimi są podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym. Projekt realizuje także cel szczegółowy Strategii, odnoszący się do rozwoju krajowego systemu cyberbezpieczeństwa poprzez ewaluację przepisów prawa dotyczących cyberbezpieczeństwa. Ponadto, projekt realizuje cele Strategii w odniesieniu do zapewnienia bezpieczeństwa łańcucha dostaw sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa. Jednocześnie wprowadzenie w życie projektowanych zmian w KSC zrealizuje kamień milowy reformy C3.1.1 KPO *Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo*.

W projekcie nałożono obowiązki na podmioty kluczowe i podmioty ważne zgodne z wykazem tych podmiotów wskazanych w załączniku nr 1 i 2 do dyrektywy NIS 2. Będą one obowiązane dokonać samorejestracji w wykazie podmiotów kluczowych i podmiotów ważnych, co umożliwi ich identyfikację, aktywne wsparcie ich przez zespoły CSIRT sektorowe i zespoły CSIRT poziomu krajowego oraz wykonywanie czynności nadzorczych przez organy właściwe do spraw cyberbezpieczeństwa. Umożliwi to także przekazywanie danych o liczbie tych podmiotów do Komisji Europejskiej i Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa.

Podmioty kluczowe i podmioty ważne będą obowiązane wprowadzić system zarządzania bezpieczeństwem informacji w procesach służących świadczeniu usług przez te podmioty. Odpowiada to zakresowi wymogów co do środków zarządzania ryzykiem wskazanych w art. 21 dyrektywy NIS 2. Tak jak do tej pory operatorzy usług kluczowych, inne podmioty kluczowe i podmioty ważne, będą obowiązane przeprowadzać audyty bezpieczeństwa swoich systemów informacyjnych co dwa lata.

Dyrektywa NIS 2 wprowadziła nowe rozwiązania w zakresie zgłaszania incydentów poważnych. Zmiany te polegają na m.in. dwuetapowym zgłaszaniu incydentu, tj. w pierwszej kolejności podmiot kluczowy albo podmiot ważny będzie zgłaszał do CSIRT sektorowego wczesne ostrzeżenie o incydencie poważnym (24 godziny od momentu wykrycia), kolejnym krokiem będzie zgłoszenie incydentu poważnego (72 godziny od momentu wykrycia). Zgłoszenie wczesnego ostrzeżenia może zawierać wniosek o wskazanie wytycznych dotyczących możliwych do wdrożenia środków ograniczających skutki incydentu poważnego lub o wsparcie techniczne przy obsłudze incydentu. CSIRT sektorowy zobowiązany będzie w terminie 24 godzin udzielić wsparcia zgodnie z treścią wniosku.

W trakcie obsługi incydentu poważnego podmiot zgłaszający incydent, na wniosek CSIRT sektorowego, przekazuje sprawozdanie okresowe z obsługi tego incydentu. Natomiast sprawozdanie końcowe z obsługi incydentu poważnego przekazywane będzie nie później niż w ciągu miesiąca od dnia zgłoszenia incydentu. Jeżeli jednak obsługa incydentu poważnego nie zakończy się w terminie miesiąca podmiot zgłaszający incydent poważny przesyła sprawozdanie z postępu obsługi incydentu, a sprawozdanie końcowe w terminie miesiąca od zakończenia obsługi tego incydentu.

Progi uznania incydentu za incydent poważny zostaną określone przez Radę Ministrów, w drodze rozporządzenia.

Zgłoszenie incydentu będzie dokonywane za pośrednictwem systemu S46. Zgodnie z projektem ustawy system S46 zostanie dostosowany do tego, by stać się głównym środkiem komunikacji pomiędzy podmiotami krajowego systemu cyberbezpieczeństwa. W związku z koniecznością dodania do tego systemu bardzo dużej liczby podmiotów zrezygnowano z zawierania porozumienia o dołączeniu do systemu. Ponadto dołączenie do systemu nie będzie już wymagało zakupu specjalnych urządzeń, ale będzie odbywało się za pomocą rozwiązań chmurowych. Podmioty kluczowe i podmioty ważne są obowiązane zapewnić zgodność swoich systemów informacyjnych z minimalnymi wymaganiami technicznymi i funkcjonalnymi podłączenia do systemu.

Projektowane rozwiązania zapewnią szybkie reagowanie na pojawiające się incydenty.

Krajowy Plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę będzie nowym dokumentem strategicznym przyjmowanym w drodze uchwały Rady Ministrów. Dokument ten będzie określał zasady postępowania w przypadku wystąpienia takiego incydentu oraz zasady współpracy między organami realizującymi zadania z zakresu cyberbezpieczeństwa oraz organami właściwymi do spraw zarządzania kryzysowego. Pozwoli to na zwiększenie efektywności działania współpracujących organów. Przyjęcie takiego dokumentu jest wymagane przez dyrektywę NIS 2.

Minister właściwy do spraw informatyzacji, w drodze postępowania administracyjnego, może uznać dostawcę produktów ICT, usług ICT lub procesów ICT za dostawcę wysokiego ryzyka. Sprzęt takiego dostawcy będzie musiał być wycofany z systemów podmiotów kluczowych i podmiotów ważnych, a nowy nie będzie mógł być wprowadzany do użytku. Pozwoli to wyeliminować potencjalnie niebezpieczny sprzęt z systemów teleinformatycznych podmiotów, których działalność jest szczególnie istotna dla funkcjonowania społeczeństwa. Wycofanie produktów ICT, usług ICT i procesów ICT dostarczanych przez dostawcę wysokiego ryzyka wiązać się może z kosztami, które będą musiały ponieść podmioty kluczowe i podmioty ważne. Nie jest jednak możliwe w tej chwili wskazanie tych kosztów, ponieważ nie można obecnie przewidzieć jaką decyzję wyda minister właściwy do spraw informatyzacji a w związku z tym jakie koszty poniosą podmioty zobowiązane do wycofania sprzętu. Należy podkreślić, że w projektowanych przepisach nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty kluczowe i podmioty ważne zostaną zobowiązane do wycofania danego sprzętu lub oprogramowania w określonym czasie.

Należy podkreślić, że przyjęcie przepisów adresujących zagrożenie wynikające z działania dostawców wysokiego ryzyka wynika z przyjętego przez państwa członkowskie Toolboxa 5G, który to dokument wymaga wprowadzenia takich środków. To podejście potwierdza także Komisja Europejska w swoim komunikacie z dnia 29 stycznia 2020 r. Komisja Europejska potwierdziła, że państwa członkowskie zgodziły się co do konieczności oceny profilu ryzyka poszczególnych dostawców i w konsekwencji stosowania odpowiednich ograniczeń wobec dostawców uznanych

za stwarzających wysokie ryzyko, w tym niezbędnych wyłączeń, aby skutecznie łagodzić ryzyko w odniesieniu do kluczowych aktywów, jak wskazano w Toolboxie[2)].

Minister właściwy do spraw informatyzacji będzie mógł wydać, w drodze decyzji administracyjnej, polecenie zabezpieczające w przypadku wystąpienia incydentu krytycznego. Zawarte w nim będzie wskazanie określonego zachowania, które zmniejszy skutki incydentu lub zapobiegnie jego rozprzestrzenianiu się. Może to być m.in. nakaz zastosowania określonej poprawki bezpieczeństwa, nakaz szczególnej konfiguracji sprzętu lub oprogramowania, zakaz korzystania z określonego sprzętu lub oprogramowania. Jednocześnie należy wskazać, że zakaz korzystania z konkretnych usług i oprogramowania będzie dotyczył wyłącznie rozwiązań mających związek z trwającym incydentem krytycznym. Takie rozwiązanie jest niezbędne, aby zapewnić skuteczną odpowiedź na wystąpienie najbardziej niebezpiecznego incydentu. W szczególności celem tego rozwiązania jest zapobiegnięcie scenariuszowi rozlewania się incydentu na kolejne sektory, np. w przypadku wystąpienia incydentu u operatora telekomunikacyjnego napastnicy mogą potencjalnie uzyskać dostęp do systemów jego klientów, wśród których mogą znajdować się szpitale czy elektrownie. Administracja musi posiadać narzędzia, które pozwolą zapobiec realizacji takiego scenariusza.

Zmiany wprowadzane projektem obejmą w dużym zakresie przepisy dotyczące nadzoru i egzekwowania przepisów. Widoczne to jest m.in. na przykładzie obecnych Operatorów Usług Kluczowych, których wyznaczono ok. 397. Dyrektywa NIS 2 obejmować będzie swoim zakresem zdecydowanie więcej podmiotów, głównie z powodu objęcia tą regulacją większej ilości sektorów. Obecnie KSC nadzór nad podmiotami krajowego systemu cyberbezpieczeństwa statuuje w art. 53, który określa organy nadzoru właściwe dla poszczególnych podmiotów oraz doprecyzowuje zakres tego nadzoru. Określone zostały również sposoby nadzoru, które w głównej mierze sprowadzają się do prowadzenia kontroli oraz nakładania kar pieniężnych na operatorów usług kluczowych i dostawców usług cyfrowych. Projektowane regulacje znacznie rozbudowują ten obszar wyposażając organy właściwe do spraw cyberbezpieczeństwa w szerokie kompetencje nadzoru i egzekwowania przepisów takie jak wydawanie ostrzeżeń, nakazów, decyzji administracyjnych nakazujących podjęcie lub zaniechanie określonego działania. Organy te zostaną również wyposażone w środki, które znajdą zastosowanie w sytuacji, w której podmiot kluczowy lub podmiot ważny nie wykonał w terminie postanowień określonych w ostrzeżeniu, nakazie czy decyzji. Wprowadza się również katalog kryteriów, które organ właściwy do spraw cyberbezpieczeństwa będzie musiał przeanalizować w celu podjęcia działań nadzorczych i egzekwowania przepisów, w tym także nakładania kar pieniężnych.

W związku z rozbudowanymi kompetencjami w powyższym zakresie, wprowadza się także możliwość stworzenia przez organ właściwy do spraw cyberbezpieczeństwa metodyki nadzoru oraz określenie hierarchii priorytetów działań nadzorczych w oparciu o metodykę i analizę ryzyka. Pozwoli to na właściwe zarządzanie swoimi obowiązkami i kompetencjami, a także prawidłowe i efektywne prowadzenie nadzoru co w konsekwencji przełoży się na wysoki poziom cyberbezpieczeństwa kraju. Powyższe zmiany związane są z kompleksowym podejściem dyrektywy NIS 2 do nadzoru ale również są wynikiem przeprowadzonej analizy obecnie obowiązujących przepisów i doświadczeń zebranych w toku ich funkcjonowania.

Nadzór wobec podmiotów kluczowych będzie miał charakter *ex ante,* a wobec podmiotów ważnych *ex post.*

Zmiana przepisów merytorycznych, w szczególności nałożenie na podmioty kluczowe i podmioty ważne nowych obowiązków i wyposażenie organów właściwych do spraw cyberbezpieczeństwa w nowe kompetencje nadzorcze, implikuje konieczność wprowadzenia szeregu zmian w przepisach o karach pieniężnych, w tym rozbudowany katalog przypadków określających, kiedy podmioty kluczowe i podmioty ważne podlegają karze pieniężnej, fakultatywne kary pieniężne nakładane na podmiot kluczowy lub podmiot ważny lub na kierownika podmiotu kluczowego lub podmiotu ważnego, zmianę wysokości kar pieniężnych, określenie formy i procedury wymierzania kar pieniężnych oraz termin jej płatności. Wprowadzona zostanie również okresowa kara pieniężna w celu przymuszenia podmiotu kluczowego lub podmiotu ważnego do realizacji nałożonych na niego obowiązków.

Oczekiwanym skutkiem wejścia w życie zaproponowanych przepisów będzie prawidłowe implementowanie do porządku krajowego przepisów dyrektywy NIS 2 w terminie do 17 października 2024 r., co wynika z art. 41 ust. 1 dyrektywy NIS 2, oraz zapewnienie sprawnego i skutecznego nadzoru nad podmiotami kluczowymi i podmiotami ważnymi, a przede wszystkim podniesienie krajowego poziomu cyberbezpieczeństwa.

Minister właściwy do spraw klimatu będzie organem właściwym w rozumieniu rozporządzenia delegowane Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

[2)] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=COM:2020:0050:FIN&_sm_au_=iVVZRW54FHZ10n2PVkFHNKt0jRsMJ.

W celu porównania zaproponowanych rozwiązań z rozwiązaniami z innych krajów wybrane zostały trzy kraje o odmiennych warunkach i położeniu geograficznym. Pierwszym z analizowanych krajów były Niemcy, duży kraj, w którym szczególnie dużo podmiotów będzie podlegało przepisom dyrektywy NIS 2. Jest to również kraj o znacznych zasobach i zdolnościach w zakresie działania w cyberprzestrzeni. Kolejnym wybranym krajem jest Belgia, która również posiada znaczne zasoby, ale jest znacznie mniejsza, co oznacza, że liczba podmiotów dotkniętych nowymi regulacjami będzie znacznie mniejsza niż w przypadku Niemiec. Wobec tego możliwa jest ocena, jak państwa o innych uwarunkowaniach podchodzą do kwestii systemu cyberbezpieczeństwa. Zdecydowano się również przeanalizować rozwiązania z innego kraju Europy Środkowo-Wschodniej, tak aby móc przeanalizować czy inna sytuacja tego regionu w polityce międzynarodowej wpływa na przyjmowane rozwiązania. Ze względu na to, że żaden z krajów tego regionu nie implementował jeszcze przepisów dotyczących NIS 2 podjęto decyzję o przeanalizowaniu rozwiązania zawartego w czeskim projekcie ustawy, który jest na zawansowanym etapie prac legislacyjnych.

W zakresie reagowania na incydenty krytyczne przeanalizowane zostały 3 kraje – Czechy, Niemcy i Włochy. Są to stosunkowo duże kraje, posiadające rozległy rynki, które często mierzą się z podobnymi problemami. Czechy, pomimo różnic wielkościowych, są z kolei krajem z Europy Środkowo-Wschodniej, co daje nam możliwość zapoznania się z perspektywą innego kraju narażonego na podobne zagrożenia jak Polska.

Niemcy

W Niemczech model nadzoru nad cyberbezpieczeństwem ma charakter scentralizowany, a zadania, w tym zakresie wykonywane są przez Federalny Urząd ds. Bezpieczeństwa Informacji (BSI), który będzie m.in. sprawował nadzór nad wszystkimi podmiotami kluczowymi i podmiotami ważnymi.
Obowiązki nałożone na podmioty kluczowe i podmioty ważne w zakresie środków mających zapewnić cyberbezpieczeństwo zostały wskazane w sposób ogólny. Mają one być zgodne z aktualnym stanem wiedzy oraz uwzględniać odpowiednie normy europejskie i międzynarodowe, koszty wdrożenia poszczególnych rozwiązań, mają także być adekwatne do oszacowanego ryzyka. Minimalne środki jakie powinny być zastosowane zostały wskazane wprost w ustawie. Status podmiotów kluczowych i podmiotów ważnych będzie nadawany z mocy samej ustawy. Podmioty spełniające wymogi ustawowe będą musiały zarejestrować się w BSI, w ciągu 3 miesięcy od wejścia w życie ustawy. Urząd może sam zarejestrować taki podmiot, jeśli nie wykona on swojego obowiązku.
Ustawa przewiduje również specjalną procedurę zwolnienia z wykonywania obowiązków określonych w ustawie dla podmiotów wykonujących zadania związane z bezpieczeństwem narodowym lub bezpieczeństwem publicznym.
Urzędy federalne muszą przeznaczać co najmniej 20% wydatków informatycznych na cyberbezpieczeństwo.
W rozporządzeniu do ustawy może być wprowadzony obowiązek korzystania z certyfikowanych produktów i usług.

Belgia

W Belgii przygotowany został projekt ustawy implementującej dyrektywę NIS 2. Przygotowana ustawa ma zastąpić dotychczasową ustawę regulującą kwestie cyberbezpieczeństwa.
Zgodnie z nową ustawą status podmiotu kluczowego i podmiotu ważnego będą posiadać z mocy prawa podmioty, które spełniają warunki określone w ustawie, będące bezpośrednim przeniesieniem przepisów dyrektywy NIS 2. Do podmiotów, które nie spełniają tych warunków, ale z innych powodów powinny być objęte regulacją, np. są jedynym dostawcą danej usługi w Belgii, pomimo niespełniania kryteriów z dyrektywy NIS 2, mogą być wydane decyzje o uznaniu ich za taki podmiot. Decyzje te wydaje krajowy organ ds. cyberbezpieczeństwa, po zasięgnięciu opinii sektorowego organu cyberbezpieczeństwa. W przypadku gdy opinia ta jest negatywna, sprawa jest kierowana do Rady Bezpieczeństwa Narodowego. Krajowy organ co dwa lata dokonuje przeglądu wydanych decyzji.
Od momentu wejścia w życie przepisów implementujących dyrektywę NIS 2 podmioty kluczowe i podmioty ważne będą miały 5 miesięcy na zarejestrowanie się w odpowiedniej bazie danych. W przypadku zmiany określonych danych, podmioty te będą miały dwa tygodnie na ich aktualizację.
Dużą rolę w ramach nowej legislacji będą miały akty wykonawcze wydawane przez króla. W takiej formie będzie przyjęty m.in. krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę.
Ustawa przewiduje również formułę dobrowolnego zgłaszania incydentów w przypadku gdy prawo nie wymaga, aby dany incydent zgłaszać, m.in. gdy podmiot, u którego incydent wystąpił nie jest podmiotem kluczowym ani podmiotem ważnym.
Ustawa określiła minimalne środki zarządzania ryzykiem w cyberbezpieczeństwie, ale to jakie dokładnie środki mają być zastosowane zależą od analizy ryzyka w konkretnym podmiocie. Odpowiedzialność za prawidłowe jej sporządzenie spoczywa na danym podmiocie.
Ustawa wyraźnie wskazuje także ogólną odpowiedzialność kierownictwa za działania, w tym zakresie i nakłada obowiązek odpowiedniego przeszkolenia wszystkich osób z kierownictwa w zakresie cyberbezpieczeństwa.

Czechy

Czeski projekt ustawy implementującej dyrektywę NIS 2 jest bardzo obszerny i zawiera rozwiązania wykraczające poza wąsko rozumiane wprowadzenie przepisów Unii Europejskiej do krajowego porządku prawnego. Projekt przewiduje utworzenie Agencji Cyberbezpieczeństwa na wzór niemieckiego BSI czy francuskiego ANSSI, która będzie zajmować się szerokim spektrum zadań z tego obszaru.
Projekt określa ogólne warunki do uznania danego podmiotu za dostawcę usług regulowanych. W zależności od rodzaju działalności dostawca usług regulowanych może być obowiązany do stosowania wysokiego reżimu cyberbezpieczeństwa albo niskiego reżimu cyberbezpieczeństwa. Jeśli dany podmiot wykonuje działalność z obu grup to wszystkie jego usługi są objęte wysokim reżimem. Na podmioty spełniające te warunki ustawa nakłada obowiązek zgłoszenia się do Agencji Cyberbezpieczeństwa w ciągu 30 dni od uzyskania wiedzy o tym. Agencja może również wpisać do wykazu tych podmiotów, te z nich o których wie, że spełniają wymagania. Projekt przewiduje również odrębny tryb wpisu do wykazu dla podmiotów spełniających odrębnie uregulowane warunki. Ten wpis będzie odbywał się na podstawie decyzji administracyjnej Prezesa Agencji. Z obowiązkiem zgłoszenia się do Agencji powiązana została sankcja karnoadministracyjna.
Dostawcy usług regulowanych mają obowiązek wdrożyć wymagane prawem rozwiązania w ciągu roku od wpisu do wykazu. Obowiązki te ujęte są bardzo ogólnie w samej ustawie, a uszczegółowione zostaną w aktach wykonawczych. Bardziej szczegółowo niż w samej dyrektywie NIS 2 zostały w nich określone środki techniczne i organizacyjne jakie mają stosować dostawcy usług regulowanych. W szczególności należy zwrócić uwagę na uregulowanie obowiązków i zadań kierownictwa podmiotów kluczowych i podmiotów ważnych. Do ich zadań należy np. informowanie pracowników o znaczeniu cyberbezpieczeństwa czy zapewniania odpowiednich zasobów do realizacji zadań z tego obszaru. Akty wykonawcze nakazują też dokonanie określonych zmian w strukturze tych podmiotów poprzez utworzenie Komitetu Zarządzania Cyberbezpieczeństwem, w którym będzie musiał zasiadać przedstawiciel kierownictwa danego podmiotu. Ponadto w akcie wykonawczym określono zakres zadań: – menadżera ds. cyberbezpieczeństwa, – architekta cyberbezpieczeństwa, – audytora cyberbezpieczeństwa i – osoby odpowiedzialnej za bezpieczeństwo zasobów i nakazano utworzyć takie stanowiska u dostawców usług regulowanych.
Agencja Cyberbezpieczeństwa może stosować środki zaradcze w postaci różnego rodzaju ostrzeżeń i środków reaktywnych. W ramach środków reaktywnych Agencja może nakazać dostawcy usług zastosowanie określonych środków, określonych w sposób ogólny, w drodze decyzji. Taki środek jest podawany do wiadomości publicznej, a ponadto Agencja informuje o nim podmioty, do których jest skierowany. Środek obowiązuje od chwili jego ogłoszenia.
Projekt przewiduje również wyłączenie stosowania przepisów o dostępie do informacji publicznej do informacji, których ujawnienie mogłoby utrudnić zapewnianie cyberbezpieczeństwa lub zmniejszać efektywność środków zaradczych.
Ustawa definiuje strategicznie ważne sektory. W odniesieniu do podmiotów, w tych sektorach, Agencja może ustanowić dodatkowe warunki dotyczące dostawców sprzętu i usług oraz zakazać stosowania sprzętu określonego dostawcy, jeśli stwierdzono, że w oparciu o kryteria ryzyka dostawców występuje znaczne zagrożenia dla bezpieczeństwa państwa, porządku wewnętrznego lub porządku publicznego.
Przewidziany został również specyficzny stan nadzwyczajny – stan cyberzagrożenia. W czasie jego trwania Agencja może wydawać rozstrzygnięcia z pominięciem przepisów o postępowaniu administracyjnym. W ramach tych rozstrzygnięć może np. zakazać stosowania określonego sprzętu przez organy administracji czy zobowiązać określone podmioty publiczne do udzielenia pomocy.
Należy zauważyć, że wszystkie projekty przewidują pewną formę samoidentyfikacji podmiotów kluczowych i podmiotów ważnych, o których mówi dyrektywa NIS 2.

Analiza w zakresie środków reagowania na incydenty krytyczne

Czechy

Czeska Agencja ds. cyberbezpieczeństwa NUKIB na podstawie sekcji 12 (1) ustawy o cyberbezpieczeństwie[3)], może wydawać ostrzeżenia do podmiotów. Ostrzeżenia wydawane są w przypadku wysokiego prawdopodobieństwa wystąpienia sytuacji kryzysowej, która może mieć krytyczne znaczenie dla bezpieczeństwa państwa. Ostrzeżenie zawiera także listę rekomendowanych działań, które podmioty powinny wdrożyć celem ograniczenia ryzyk związanych z sytuacją kryzysową. Przykłady rekomendacji: zwrócenie uwagi na określony typ cyberataków np. spear-phishingów, potrzebie zablokowania dostępu do swojej infrastruktury IT, pilnej konieczności dokonania aktualizacji oprogramowania, czy też zwrócenie szczególnej uwagi na wskazane w ostrzeżeniu domeny. Przykładem takiego ostrzeżenia jest dokument wydany 16 kwietnia 2020 r. znak 2066/2020-NÚKIB-E/350. Na podstawie analizy możliwych

[3)] Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) https://www.zakonyprolidi.cz/cs/2014-181.

zagrożeń NUKIB wydał ostrzeżenie dla całego państwa, ze szczególnym naciskiem na sektor ochrony zdrowia[4]. Innym przykładem jest ostrzeżenie NUKIB z 25 lutego 2022 r. znak 2384/2022-NÚKIB-E/350 wskazujące na cyberzagrożenia o charakterze krytycznym, którego wystąpienie w systemach czeskiej administracji publicznej czy innych organizacji strategicznych jest bardzo prawdopodobne[5].

Niemcy

Niemiecki Federalny Urząd Bezpieczeństwa Teleinformatycznego (Bundesamt für. Sicherheit in der Informationstechnik – BSI) może, na podstawie § 7 BSI-Gesetz[6] ogłaszać ostrzeżenia o: podatnościach w produktach i usługach informatycznych, złośliwym oprogramowaniu, utracie lub nieautoryzowanym dostępie do danych, a także zalecać środki bezpieczeństwa.

Włochy

We Włoszech dekret nr 105 z 21 września 2019 r.[7] uprawnia Prezesa Rady Ministrów do nakazania całkowitego lub częściowego wycofania z eksploatacji jednego lub więcej urządzeń lub produktów, w sytuacji poważnego i bezpośredniego zagrożenia bezpieczeństwa narodowego związanego z podatnościami występującymi w sieciach, systemach i usługach. Środek ten może być stosowany, jeżeli zagrożenia nie można uniknąć w inny sposób i tylko przez czas ściśle niezbędny do wyeliminowania lub ograniczenia konkretnego ryzyka.

Analiza w zakresie dostawców wysokiego ryzyka

Projektodawca przy projektowaniu przepisów prawa dotyczących uznania dostawców sprzętu lub oprogramowania za dostawców wysokiego ryzyka – czyli wdrożenia zaleceń z tzw. 5G Toolbox, dokonał analizy porównawczej rozwiązań prawno-organizacyjnych zaimplementowanych lub zaproponowanych mechanizmów. Wyniki analizy zostały zaprezentowane w załączniku nr 1 do OSR *Dostawca wysokiego ryzyka (high risk vendor) i bezpieczeństwo sieci 5G w Europie*.

W większości państw Unii Europejskiej wprowadzone zostały przepisy umożliwiające wyłączenie z budowy sieci 5G dostawcy uznanego za potencjalne zagrożenie dla bezpieczeństwa narodowego. Obowiązujące regulacje przewidują dokonanie takiego wyłączenia w drodze władczego rozstrzygnięcia dokonywanego przez jeden z organów władzy wykonawczej np. w drodze decyzji administracyjnej. W wielu państwach w tego rodzaju postępowaniach istotną rolę odgrywa również organ doradczy składający się z przedstawicieli administracji, wojska oraz służb specjalnych.

4. Podmioty, na które oddziałuje projekt

W przypadku liczby podmiotów kluczowych i podmiotów ważnych źródłem danych są *Tablice dotyczące podmiotów gospodarki narodowej zarejestrowanych w rejestrze REGON deklarujących prowadzenie działalności według stanu na31 grudnia 2023 r.*[8], chyba że wskazano inne źródło. Korzystając z REGON przyjęto dane o liczbie podmiotów, które zatrudniają co najmniej 50 pracowników, nie brano przy tym pod uwagę danych o obrocie i bilansie. Ze względu na brak dokładnych danych, a także niewystarczającą dokładność kodów PKD m. in. w sektorze infrastruktury cyfrowej, zarządzania ICT czy dostawców usług cyfrowych należy traktować te dane jako dane szacunkowe. Część podmiotów świadczy zróżnicowane usługi, przekraczające zakres pojedynczego sektora z dyrektywy NIS 2. Ponadto z uwagi na bieżące życie gospodarcze liczba podmiotów w poszczególnych sektorach ciągle się zmienia, tworzone są nowe podmioty, a dotychczasowe są przekształcane oraz likwidowane. Liczba podmiotów w OSR będzie podlegała aktualizacji w toku procesu legislacyjnego, stosownie do posiadanych danych.

Grupa	Wielkość	Źródło danych	Oddziaływanie
Centrum e-Zdrowie	1	Informacja ogólnodostępna	Z dniem wejścia w życie ustawy stanie się zespołem CSIRT sektorowym.

[4] https://www.nukib.cz/download/publications_en/Warning-NUKIB-2020-04-16.pdf.

[5] https://nukib.cz/download/aktuality/2021-01-17_varovani_v.1.7_EN.pdf.

[6] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html.

[7] Decreto-legge 21 settembre 2019, n. 105 Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica. https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg.

[8] https://stat.gov.pl/obszary-tematyczne/podmioty-gospodarcze-wyniki-finansowe/zmiany-strukturalne-grup-podmiotow/kwartalna-informacja-o-podmiotach-gospodarki-narodowej-w-rejestrze-regon-rok-2023,7,13.html.

CSIRT KNF	1	Informacja ogólnodostępna	Z dniem wejścia w życie ustawy stanie się zespołem CSIRT sektorowym.
CSIRT NASK	1	Informacja ogólnodostępna	Z dniem wejścia w życie ustawy stanie się zespołem CSIRT sektorowym.
Kolegium do spraw Cyberbezpieczeństwa	1	Informacja ogólnodostępna	Kolegium otrzyma nowe kompetencje w postaci wydawania opinii o dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa.
Minister Obrony Narodowej	1	Informacja ogólnodostępna	Będzie pełnił rolę organu ds. zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę w zakresie w jakim dotyczy to obronności i Sił Zbrojnych.
Minister właściwy do spraw informatyzacji	1	Informacja ogólnodostępna	Będzie pełnił rolę organu ds. zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę. Obowiązek utworzenia wykazu podmiotów kluczowych i podmiotów ważnych.
Organy właściwe do spraw cyberbezpieczeństwa – Komisja Nadzoru Finansowego Minister Obrony Narodowej minister właściwy do spraw energii minister właściwy do spraw gospodarki minister właściwy do spraw gospodarki morskiej minister właściwy do spraw gospodarki wodnej minister właściwy do spraw informatyzacji minister właściwy do spraw klimatu minister właściwy do spraw nauki i szkolnictwa wyższego minister właściwy do spraw rolnictwa minister właściwy do spraw transportu	14	Informacja ogólnodostępna	Wyposażenie w uprawnienia i obowiązki w związku ze sprawowaniem nadzoru nad podmiotami kluczowymi i podmiotami ważnymi.

minister właściwy do spraw zdrowia Prezes UKE			
Szefa Krajowej Administracji Skarbowej	1	Informacja ogólnodostępna	Na żądanie organu właściwego do spraw Cyberbezpieczeństwa będzie przekazywał informacje niezbędne do ustalenia wielkości przedsiębiorcy – podmiotu kluczowego/ważnego.
Zakład Ubezpieczeń Społecznych	1	Informacja ogólnodostępna	Na żądanie organu właściwego do spraw Cyberbezpieczeństwa będzie przekazywał informacje niezbędne do ustalenia wielkości przedsiębiorcy – podmiotu kluczowego/ważnego.
Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa	1	Informacja ogólnodostępna	Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa będzie mógł wydawać rekomendacje, nakazywać CSIRT poziomu krajowego wsparcie w obsłudze incydentów konkretnym podmiotom krajowego systemu cyberbezpieczeństwa. Będzie mógł także żądać od administracji rządowej informacji i dokumentów niezbędnych do wykonywania jego zadań, a także otrzyma możliwość zlecania niezbędnych badań. Pełnomocnikiem z mocy ustawy będzie minister właściwy do spraw informatyzacji, sekretarz stanu albo podsekretarz stanu w urzędzie obsługującym ministra właściwego do spraw informatyzacji.
Podmioty kluczowe i podmioty ważne z podsektora produkcji wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro	44	REGON PKD sekcja C dział 32 podklasa 3250z	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.

Podmioty kluczowe i podmioty ważne z sektora administracji publicznej	27905	REGON	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
Podmioty ważne z sektora badań naukowych	169	REGON PKD sekcja M dział 72 podklasa: 7219Z Badania naukowe i prace rozwojowe w dziedzinie pozostałych nauk przyrodniczych i technicznych 7220Z Badania naukowe i prace rozwojowe w dziedzinie nauk społecznych i humanistycznych	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
Podmioty kluczowe i podmioty ważne z sektora bankowości i infrastruktury rynków finansowych	547	szacunki od KNF	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
Podmioty kluczowe i podmioty ważne z sektora dostawców usług cyfrowych	Ok. 40	Szacunki Ministerstwa Cyfryzacji	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
Podmioty kluczowe i podmioty ważne z sektora energii	365	Szacunki od Ministerstwa Klimatu i Środowiska	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.

Podmioty ważne z sektora gospodarowania odpadami	276	REGON PKD: Sekcja E dział 38 podklasa 3811Z Zbieranie odpadów innych niż niebezpieczne Sekcja E dział 38 podklasa 3812Z Zbieranie odpadów niebezpiecznych Sekcja E dział 38 podklasa 3821Z Obróbka i usuwanie odpadów innych niż niebezpieczne Sekcja E dział 38 podklasa 3822Z Przetwarzanie i unieszkodliwianie odpadów niebezpiecznych Sekcja E dział 38 podklasa 3831Z Demontaż wyrobów zużytych Sekcja E dział 38 podklasa 3832Z Odzysk surowców z materiałów segregowanych Sekcja E dział 38 podklasa 3900Z Działalność związana z rekultywacją i pozostała działalność usługowa związana z gospodarką odpadami	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
Podmioty kluczowe i podmioty ważne z sektora infrastruktury cyfrowej z wyłączeniem podsektora komunikacji elektronicznej	462	Szacunki Ministerstwa Cyfryzacji	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
Podmioty kluczowe i podmioty ważne z podsektora komunikacji elektronicznej	3784	Rejestr przedsiębiorców telekomunikacyjnych; w zakresie podmiotów świadczących usługę komunikacji interpersonalnej niewykorzystującej numerów (OTT-1) brak danych	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
Podmioty ważne z sektora poczty	280	Rejestr operatorów pocztowych	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania

			incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
Podmioty kluczowe i podmioty ważne z sektora produkcja, przetwarzanie i dystrybucja żywności	1204	REGON PKD: sekcja C dział 10 Produkcja artykułów spożywczych Sekcja H dział 46 podklasa 4631Z Sprzedaż hurtowa owoców i warzyw Sekcja H dział 46 podklasa 4632Z Sprzedaż hurtowa mięsa i wyrobów z mięsa Sekcja H dział 46 podklasa 4633Z Sprzedaż hurtowa mleka, wyrobów mleczarskich, jaj, olejów i tłuszczów jadalnych Sekcja H dział 46 podklasa 4634A Sprzedaż hurtowa napojów alkoholowych Sekcja H dział 46 podklasa 4634B Sprzedaż hurtowa napojów bezalkoholowych	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
Podmioty kluczowe i podmioty ważne z sektora produkcja, wytwarzanie i dystrybucja chemikaliów	214	REGON PKD sekcja C dział 20 Produkcja chemikaliów i wyrobów chemicznych	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
Podmioty kluczowe i podmioty ważne z sektora produkcji, z wyłączeniem wyrobów medycznych	1120	REGON PKD sekcja C dział 26 Produkcja komputerów, wyrobów elektronicznych i optycznych PKD sekcja C dział 27 Produkcja urządzeń elektrycznych PKD sekcja C dział 28 Produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana PKD sekcja C dział 29 Produkcja pojazdów	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.

		samochodowych, przyczep i naczep, z wyłączeniem motocykli PKD sekcja C dział 30 Produkcja pozostałego sprzętu transportowego	
Podmioty kluczowe i podmioty ważne z sektora ścieków	102	REGON PKD sekcja E dział 37 podklasa 3700z Odprowadzanie i oczyszczanie ścieków	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
Podmioty kluczowe i podmioty ważne z sektora transportu	Co najmniej 450	Szacunki od Ministerstwa Infrastruktury	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
Podmioty kluczowe i podmioty ważne z sektora transportu wodnego	11	REGON	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
Podmioty kluczowe i podmioty ważne z sektora wody pitnej	268	REGON PKD Sekcja E dział 36 podklasa 3600Z Pobór, uzdatnianie i dostarczanie wody	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
Podmioty kluczowe i podmioty ważne z sektora zarządzania ICT	43	REGON PKD sekcja J dział 62 podklasa 6203z Działalność związana z zarządzaniem urządzeniami informatycznymi	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania

		W zakresie dostawców usług zarządzanych w zakresie cyberbezpieczeństwa źródłem informacji są dane ENISA[9)]	produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
Podmioty kluczowe i podmioty ważne z sektora zdrowia	1248	REGON PKD Dział 21 Produkcja podstawowych substancji farmaceutycznych oraz leków i pozostałych wyrobów farmaceutycznych PKD Dział 86 Opieka zdrowotna PKD sekcja M dział 72 podklasa 7211Z Badania naukowe i prace rozwojowe w dziedzinie biotechnologii Rozporządzenie Ministra Zdrowia z dnia 19 czerwca 2012 r. w sprawie wykazu laboratoriów referencyjnych	Nowe obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki zgłaszania incydentów do właściwych CSIRT sektorowych. Obowiązek wycofania produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka.
sądy administracyjne			Rozpatrywanie skarg na decyzje o nałożeniu administracyjnej kary pieniężnej na podmiot kluczowy albo podmiot ważny.
Szef Agencji Wywiadu	1	Informacja ogólnodostępna	Pozytywne. Szef Agencji Wywiadu będzie mógł uczestniczyć w posiedzeniach Kolegium do Spraw Cyberbezpieczeństwa, a tym samym współtworzyć opinie Kolegium, dzięki czemu będą uwzględnione wszystkie aspekty cyberbezpieczeństwa i bezpieczeństwa narodowego.
Szef Centralnego Biura Antykorupcyjnego	1	Informacja ogólnodostępna	Pozytywne. Szef Centralnego Biura Antykorupcyjnego będzie mógł uczestniczyć w posiedzeniach Kolegium do Spraw Cyberbezpieczeństwa, a tym samym współtworzyć opinie Kolegium, dzięki czemu będą uwzględnione wszystkie aspekty cyberbezpieczeństwa

[9)] https://www.enisa.europa.eu/topics/incident-response/csirt-inventory/certs-by-country-interactive-map.

			i bezpieczeństwa narodowego.
Szef Służby Wywiadu Wojskowego	1	Informacja ogólnodostępna	Pozytywne. Szef Służby Wywiadu Wojskowego będzie mógł uczestniczyć w posiedzeniach Kolegium do Spraw Cyberbezpieczeństwa, a tym samym współtworzyć opinie Kolegium, dzięki czemu będą uwzględnione wszystkie aspekty cyberbezpieczeństwa i bezpieczeństwa narodowego.
Szef Agencji Bezpieczeństwa Wewnętrznego	1	Informacja ogólnodostępna	Będzie pełnił rolę organu właściwego do spraw cyberbezpieczeństwa w sektorze administracji publicznej.
Konsumenci			Większy poziom bezpieczeństwa dostarczanych produktów i usług.
Urząd Dozoru Technicznego	1		Urząd Dozoru Technicznego będzie pełnił funkcję CSIRT sektorowego dla sektorów produkcji, produkcji chemikaliów i przestrzeni kosmicznej.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248 oraz z 2024 r. poz. 757), projekt został udostępniony w Biuletynie Informacji Publicznej Ministerstwa Cyfryzacji.

Ponadto zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2024 r. poz. 806), projekt został udostępniony również w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

W ramach 30-dniowych konsultacji publicznych projekt został skierowany do następujących podmiotów:
1) Amerykańskiej Izby Handlowej;
2) Business Centre Club;
3) Federacji Konsumentów;
4) Fundacji Bezpieczna Cyberprzestrzeń;
5) Fundacji ePaństwo;
6) Fundacji im. Stefana Batorego;
7) Fundacji Instytut Mikromakro;
8) Fundacji My Pacjenci;
9) Fundacji Nowoczesna Polska;
10) Fundacji Panoptykon;
11) Fundacji Projekt Polska;
12) Fundacji Przedsiębiorców Polskich Archiwizjoner;
13) Fundacji Pułaskiego;
14) Green Rev Institute;
15) Internet Society Poland Chapter;
16) Internet Society Poland;
17) ISAC-GIG;
18) ISAC-Kolej;

19) ISAC-Lotniczy;
20) Izby Domów Maklerskich;
21) Izby Gospodarczej Towarzystw Emerytalnych;
22) Izby Gospodarki Elektronicznej;
23) Konfederacji Lewiatan;
24) Krajowego Związku Banków Spółdzielczych;
25) Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji;
26) Krajowej Izby Gospodarczej;
27) Krajowej Izby Gospodarki Cyfrowej;
28) Krajowej Izby Gospodarki Morskiej;
29) Krajowej Izby Komunikacji Ethernetowej;
30) Krajowej Izby Rozliczeniowej;
31) Krajowej Spółdzielczej Kasy Oszczędnościowo-Kredytowej;
32) Naczelnej Organizacji Technicznej;
33) Naczelnej Rady Zrzeszeń Handlu i Usług;
34) Ogólnopolskiego Porozumienia Organizacji Radioamatorskich;
35) Polskiego Centrum Badań i Certyfikacji S.A.;
36) Polskiego Stowarzyszenia Marketingu SMB;
37) Polskiego Towarzystwa Informatycznego;
38) Polskiego Związku Krótkofalowców;
39) Polskiej Izby Brokerów Ubezpieczeniowych i Reasekuracyjnych;
40) Polskiej Izby Handlu;
41) Polskiej Izby Informatyki i Telekomunikacji;
42) Polskiej Izby Komunikacji Elektronicznej;
43) Polskiej Izby Producentów Urządzeń i Usług na rzecz Kolei;
44) Polskiej Izby Radiodyfuzji Cyfrowej;
45) Polskiej Izby Ubezpieczeń;
46) Polskiej Organizacji Handlu i Dystrybucji;
47) Polskiej Organizacji Niebankowych Instytucji Płatności;
48) Polskiej Rady Biznesu;
49) Polskiej Wytwórni Papierów Wartościowych;
50) Sektorowej Rady ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo;
51) Stowarzyszenia Inżynierów Telekomunikacji;
52) Stowarzyszenia Polskich Brokerów Ubezpieczeniowych i Reasekuracyjnych;
53) Towarzystwa Gospodarczego Polskie Elektrownie;
54) Związku Banków Polskich;
55) Związku Importerów i Producentów Sprzętu Elektrycznego i Elektronicznego Branży RTV i IT – ZIPSEE „Cyfrowa Polska”;
56) Związku Pracodawców Branży Internetowej IAB Polska;
57) Związku Pracodawców Mediów Elektronicznych i Telekomunikacji Mediakom;
58) Związku Pracodawców Mediów Publicznych;
59) Związku Przemysłu Motoryzacyjnego;
60) Związku Telewizji Kablowych w Polsce Izba Gospodarcza.

<u>W ramach 30-dniowego opiniowania projekt został skierowany do następujących podmiotów:</u>
1) Agencji Bezpieczeństwa Wewnętrznego;
2) Agencji Wywiadu;
3) Biura Bezpieczeństwa Narodowego;
4) Centralnego Biura Antykorupcyjnego;
5) Komisji Nadzoru Finansowego;
6) Krajowej Rady Radiofonii i Telewizji;
7) Najwyższej Izby Kontroli;
8) Polskiego Komitetu Normalizacyjnego;
9) Prezesa Głównego Urzędu Statystycznego;
10) Prezesa Urzędu Komunikacji Elektronicznej;
11) Prezesa Urzędu Ochrony Danych Osobowych;
12) Prezesa Urzędu Ochrony Konkurencji i Konsumentów;
13) Prokuratorii Generalnej Rzeczypospolitej Polskiej;
14) Rady Dialogu Społecznego;
15) Rządowego Centrum Bezpieczeństwa;

16) Rzecznika Małych i Średnich Przedsiębiorców;
17) Rzecznika Praw Obywatelskich;
18) Służby Kontrwywiadu Wojskowego;
19) Służby Ochrony Państwa;
20) Służby Wywiadu Wojskowego;
21) Urzędu Zamówień Publicznych;
22) Wojskowego Biura Zarządzania Częstotliwościami.

Wyniki ww. procesów zostały omówione w raporcie z konsultacji.

Projekt zostanie przekazany również do opinii Komisji Wspólnej Rządu i Samorządu Terytorialnego.

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	0	54,517	65,731	71,496	77,664	84,266	90,995	98,055	105,728	114,295	122,537	885,284
budżet państwa	0	7,837	10,428	11,738	13,139	14,639	16,244	17,961	19,798	21,765	23,869	157,418
JST	0	7,837	10,428	11,738	13,139	14,639	16,244	17,961	19,798	21,765	23,869	157,418
Fundusz Pracy	0	1,006	1,076	1,152	1,232	1,319	1,411	1,510	1,616	1,729	1,850	13,900
FS	0	1,458	1,560	1,670	1,787	1,912	2,046	2,189	2,343	2,507	2,683	20,155
FUS	0	28,569	33,170	35,495	37,984	40,646	43,496	46,545	49,808	53,299	57,035	426,047
NFZ	0	7,81	9,07	9,70	10,38	11,11	11,55	11,89	12,36	13,23	13,23	110,34
Wydatki ogółem	0	307,471	322,132	341,530	371,967	405,787	444,975	463,092	505,289	554,727	615,319	4332,289
budżet państwa	0	307,471	322,132	341,530	371,967	405,787	444,975	463,092	505,289	554,727	615,319	4332,289
JST	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Pracy	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Solidarnościowy	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Ubezpieczeń Społecznych	0	0	0	0	0	0	0	0	0	0	0	0
Narodowy Fundusz Zdrowia	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	0	-252,954	-256,402	-270,034	-294,303	-321,521	-353,980	-365,037	-399,561	-440,432	-492,782	-3447,005
budżet państwa	0	-299,633	-311,704	-329,792	-358,828	-391,148	-428,731	-445,131	-485,491	-532,962	-591,450	-4174,871
JST	0	7,837	10,428	11,738	13,139	14,639	16,244	17,961	19,798	21,765	23,869	157,418
Fundusz Pracy	0	1,006	1,076	1,152	1,232	1,319	1,411	1,510	1,616	1,729	1,850	13,900
Fundusz Solidarnościowy	0	1,458	1,560	1,670	1,787	1,912	2,046	2,189	2,343	2,507	2,683	20,155
Fundusz Ubezpieczeń Społecznych	0	28,569	33,170	35,495	37,984	40,646	43,496	46,545	49,808	53,299	57,035	426,047
Narodowy Fundusz Zdrowia	0	7,810	9,067	9,703	10,383	11,111	11,554	11,890	12,364	13,231	13,231	110,345

Źródła finansowania	Budżet państwa w częściach: • 16 Kancelaria Prezesa Rady Ministrów • 20 gospodarka • 21 gospodarka morska • 22 gospodarka wodna • 27 informatyzacja • 28 szkolnictwo wyższe i nauka

	• 32 rolnictwo • 39 transport • 46 zdrowie • 47 energia • 51 klimat • 57 Agencja Bezpieczeństwa Wewnętrznego • 76 Urząd Komunikacji Elektronicznej Jako rok 1 przyjęto rok 2025 – pierwszy pełny kalendarzowy rok funkcjonowania ustawy. Zadania przewidziane w projekcie są zadaniami nowymi, które do tej pory nie były planowane w budżecie państwa, stąd też jest zasadne zwiększenie limitów wydatków w poszczególnych częściach budżetowych. Ewentualne skutki dla części 05 – *Naczelny Sąd Administracyjny* wynikające z wejścia w życie projektowanej ustawy zostaną sfinansowane w ramach dotychczasowych środków finansowych i nie będą stanowić podstawy do planowania oraz ubiegania się o dodatkowe środki z budżetu państwa w roku wejścia w życie ustawy oraz w latach kolejnych. Wszystkie skutki finansowe z tytułu realizacji projektowanej ustawy w części 46 – *Zdrowie* sfinansowane zostaną w ramach środków na ochronę zdrowia, w tym w ramach ustalonego funduszu wynagrodzeń (niezwiększonego z tytułu tej ustawy), określonych zgodnie z art. 131c ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2024 r. poz. 146, z późn. zm.), bez możliwości ubiegania się o dodatkowe środki ponad te kwoty. W tabeli powyżej przedstawiono dochody i wydatki w milionach zł zaokrąglone do 3 miejsc po przecinku. Szczegółowe wykazanie wydatków bez zaokrąglenia znajduje się w załączniku nr 4 do OSR.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	**Wsparcie kadrowe organów właściwych do spraw cyberbezpieczeństwa w realizacji zadań nadzorczych nad podmiotami kluczowymi i podmiotami ważnymi** Projektowane zmiany mają zapewnić odpowiedni poziom finansowania działalności organów właściwych ds. cyberbezpieczeństwa. Wspomniany poziom musi być adekwatny do zadań nałożonych na te organy wymaganiami procedowanej ustawy oraz dyrektywy NIS 2. Obecny poziom finansowania nie pozwala na zatrudnienie wystarczającej liczby specjalistów w stosunku do liczby obowiązków, a także liczby podmiotów jakie będą objęte nadzorem organów właściwych do spraw cyberbezpieczeństwa wraz z wejściem w życie przedmiotowej regulacji. Dodatkowo poprzez zwiększanie finansowania zostanie zapewniona nie tylko większa liczba etatów niezbędnych do efektywnej realizacji zadań organu właściwego ds. cyberbezpieczeństwa, ale także zostanie zapewniona możliwość zaoferowania wynagrodzeń, które będą adekwatne i proporcjonalne do realiów panujących w sektorze prywatnym oraz do wymaganej wiedzy i umiejętności. Obecnie obowiązująca KSC zapewnia finansowanie na poziomie 789 000,00 zł rocznie, co na dzień wejścia ustawy w życie miała zapewnić – stworzenie 8 stanowisk pracy przy założeniach, że dla 1 etatu przyjęto mnożnik kwoty bazowej w wysokości 3,20, przy maksymalnym 20% dodatku stażowym. Dodatkowo, założenie obejmowało również trzynaste wynagrodzenie roczne. Jednakże powyższe obliczenia były realizowane dla kwoty bazowej wynoszącej 1 874,00 zł. Przez ostatnie lata kwota bazowa ulegała zwiększeniu i obecnie wynosi ona 2 628,54 zł, co powoduje, że pierwotne założenia dotyczące maksymalnego wynagrodzenia oraz liczby stanowisk pracy, jakie miały być zapewnione – są nieaktualne. W dotychczasowej kwocie nie założono wzrostu kwoty bazowej przy zapewnieniu finansowania, co powinno zostać zmienione w powstającej regulacji. Dodatkowo dyrektywa NIS 2 w sposób diametralny zmienia metodę wyznaczania podmiotów, które zostaną objęte nadzorem organów właściwych do spraw cyberbezpieczeństwa oraz zakres podmiotowy regulacji, powodujący znaczny wzrost liczby tych podmiotów czy też znacznie zwiększa zakres obowiązków realizowanych przez organy właściwe, co również przekłada się na konieczność zapewnienia odpowiednich zasobów kadrowych. Zgodnie z przepisami zawartymi w dyrektywie NIS 2 pojawia się zasada, która wskazuje, że przedsiębiorstwa automatycznie zostaną uznane za kluczowe lub ważne w procesie samoidentyfikacji, po spełnieniu kryteriów dla średniego przedsiębiorstwa wskazanych w art. 2 załącznika do zalecenia 2003/361/WE, w związku z tym, podmiotami kluczowymi będą podmioty z sektorów, o których mowa w załączniku nr I KSC, przekraczające pułapy dla średnich

	przedsiębiorców. Natomiast, podmioty ważne to podmioty z sektorów wymienionych w załączniku nr I lub nr II, które nie kwalifikują się jako podmioty kluczowe. W związku z tym, że główne zadania organu właściwego ds. cyberbezpieczeństwa skupiają się na czynnościach nadzorczych, w tym zadaniach kontrolnych, przyjęto następujące założenia do obliczenia wymaganej liczby pracowników, którzy będą realizować te zadania. Założono, że rocznie należy przeprowadzić kontrolę około 10% nadzorowanych podmiotów (kontrola o charakterze *ex-ante* lub *ex-post*). Zespół kontrolny liczący 3 osoby jest w stanie przeprowadzić około 6 kontroli rocznie. W przypadku sektorów, gdzie jest znikoma liczba podmiotów, może to być mniejsza liczba osób. Założono przy tym, że niezależnie od wielkości sektora, maksymalna liczba nowych etatów nadzorujących sektor to 40 etatów. Należy podkreślić, że działania kontrolne są jednymi z wielu zadań wynikających z dyrektywy NIS 2, a co za tym idzie, wymienione wyżej zespoły kontrolne będą okresowo wyłączane z czynności kontrolnych, na rzecz innych działań. Oprócz czynności kontrolnych, niektóre inne kompetencje organu właściwego ds. cyberbezpieczeństwa to: 1) prowadzenie bieżącej analizy podmiotów w danym sektorze lub podsektorze pod kątem uznania ich za podmiot kluczowy lub podmiot ważny; 2) wpisywanie z urzędu podmiotów kluczowych lub podmiotów ważnych do wykazu podmiotów kluczowych i podmiotów ważnych; 3) monitorowanie stosowania przepisów ustawy przez podmioty kluczowe i podmioty ważne; 4) wzywanie na wniosek CSIRT MON, CSIRT NASK lub CSIRT GOV podmiotów kluczowych i podmiotów ważnych do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu poważnego lub krytycznego; 5) w uzasadnionych przypadkach współpraca z organami ścigania i organem właściwym do spraw ochrony danych osobowych; 6) przygotowywanie we współpracy z CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowymi zespołami cyberbezpieczeństwa rekomendacji dotyczących działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów; 7) nakładanie administracyjnych kar pieniężnych. W związku z powyższym należy zapewnić finansowanie działania organu właściwego ds. cyberbezpieczeństwa na poziomie wystarczającym do niezakłóconego i efektywnego realizowania zadań, które bezpośrednio przełożą się na cyberbezpieczeństwo sektorów. Kwota powinna być systematycznie zwiększana w kolejnych latach. Dla 1 etatu przyjęto maksymalny mnożnik kwoty bazowej w wysokości 4,0, przy maksymalnym 20% dodatku stażowym. Powyższy mnożnik maksymalny został ustalony na podstawie następujących założeń. Zgodnie z obwieszczeniem Prezesa Głównego Urzędu Statystycznego z dnia 22 stycznia 2024 r. w sprawie przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw w grudniu 2023 r. przeciętne miesięczne wynagrodzenie w sektorze przedsiębiorstw wyniosło 8 032,96 zł. Dodatkowo, jak wynika z Raportu Płacowego 2023 r. udostępnionego przez Organizację Pracodawców Usług IT – SoDA, średnia pensja specjalisty IT to 11 427,00 zł brutto. Uśredniona wartość wynagrodzenia IT jest więc o ponad 4 tys. wyższa niż mediana zarobków w kraju. W związku z powyższym założono, że oferowane wynagrodzenie powinno być wyższe od średniego wynagrodzenia w sektorze prywatnym (średnia ze wszystkich branż gospodarki), jednak mieszczące się w uśrednionej wartości wynagrodzenia w branży IT w 2023 r. Ponadto zaproponowany mnożnik maksymalny został ustalony na takim poziomie, który daje możliwość pozyskania wysoko wykwalifikowanej kadry posiadającej specjalistyczną wiedzę. Należy ponownie podkreślić, że pozyskanie specjalistów z sektora prywatnego wymaga zaoferowania stawek konkurencyjnych względem tego właśnie sektora. Dodatkowo rekomenduje się rozwiązanie, które pozwoli zniwelować problem niewystarczającego poziomu finansowania w przypadku wzrostu kosztów zatrudnienia związanego z m.in. wzrostem kwoty bazowej czy wzrostem średniego wynagrodzenia w gospodarce w kolejnych 10 latach. Takiego mechanizmu zabrakło w obowiązującej KSC, co spowodowało część opisanych wyżej problemów. Określenie tego, w jaki sposób będzie kształtowała się kwota bazowa lub średnie wynagrodzenie w kolejnych 10 latach, jest bardzo trudne. Wobec powyższego przyjęto mechanizm, który pozwoli oszacować wspomniany wzrost, bazując na danych historycznych.

Do prognozowania skutków finansowych ustawy dla kolejnych 10 lat wraz z uwzględnieniem konieczności wzrostu tego finansowania bazowano na danych historycznych z Zakładu Ubezpieczeń Społecznych.

ROK	ŚREDNIE WYNAGRODZENIE w GOSPODARCE KRAJOWEJ	PROCENT WZROSTU
2013	3650,06	
2014	3783,46	3,65 %
2015	3899,78	3,07%
2016	4047,21	3,78 %
2017	4271,51	5,54%
2018	4585,03	7,34%
2019	4918,17	7,27%
2020	5167,47	5,07%
2021	5662,53	9,58%
2022	6346,15	12,07%
2023	7155,48	12,75%

Na podstawie powyższych danych można ustalić, że wzrost przeciętnego wynagrodzenia w gospodarce krajowej w ciągu ostatnich 10 lat wyniósł średnio 7,01%. W związku z tym proponuje się przyjąć prognozę analogicznego wzrostu przeciętnego wynagrodzenia w gospodarce w prognozie na kolejne 10 lat.

O wartość 7,01% w każdym kolejnym roku zostanie powiększona kwota finansowania organu właściwego ds. cyberbezpieczeństwa, co powinno zapewnić wystarczające środki finansowe w obliczu powiększania się kwoty bazowej w administracji, ale także pozwoli na zapewnienie konkurencyjności wynagrodzeń w stosunku do zwiększającego się przeciętnego wynagrodzenia w gospodarce krajowej w sektorze prywatnym.
Wzrost finansowania organów właściwych do spraw cyberbezpieczeństwa o 7,0% w każdym roku jest zasadny i konieczny, aby zapewnić odpowiedni poziom kadry, bowiem dyrektywa NIS 2 nakazuje państwom członkowskim wprowadzenie efektywnego nadzoru nad podmiotami kluczowymi i podmiotami ważnymi – aby to zrealizować organy właściwe do spraw cyberbezpieczeństwa potrzebują niezbędnej kadry. Obniżenie poziomu finansowania może spowodować ryzyko odpływu doświadczonych pracowników do sektora prywatnego, ponieważ nie zostaną zapewnione dla nich odpowiednie warunki finansowe. Ponadto, nieadekwatne wynagrodzenie nie przyciągnie kandydatów z rynku, co spowoduje nieskuteczność kadry organów właściwych do spraw cyberbezpieczeństwa.

Podsumowanie nowych etatów		
Sektor/podsektor	**Organ właściwy do spraw cyberbezpieczeństwa**	**Nowe etaty**
Energia	minister właściwy do spraw energii	19
Transport wodny	minister właściwy do spraw gospodarki morskiej	1
Transport	minister właściwy do spraw transportu	23
Bankowość i infrastruktura rynków finansowych	Komisja Nadzoru Finansowego	28
Zdrowie	minister właściwy do spraw zdrowia	40
Woda pitna	minister właściwy do spraw gospodarki wodnej	14
Ścieki	minister właściwy do spraw gospodarki wodnej	6
Infrastruktura Cyfrowa	minister właściwy do spraw informatyzacji	24
Dostawcy usług cyfrowych	minister właściwy do spraw informatyzacji	2

Komunikacja elektroniczna	Prezes UKE	40
Zarządzanie ICT	minister właściwy do spraw informatyzacji	3
Administracja publiczna z wyłączeniem MON i służb specjalnych	minister właściwy do spraw informatyzacji	40
Przestrzeń kosmiczna	minister właściwy do spraw gospodarki	0
Poczta	Prezes UKE	14
Gospodarowanie odpadami	minister właściwy do spraw klimatu	14
Produkcja, wytwarzanie i dystrybucja chemikaliów	minister właściwy do spraw gospodarki	11
Produkcja, przetwarzanie i dystrybucja żywności	minister właściwy do spraw rolnictwa	40
Produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro	minister właściwy do spraw zdrowia	3
Produkcja ogółem z wyłączeniem wyrobów medycznych	minister właściwy do spraw gospodarki	40
Badania naukowe	minister właściwy do spraw nauki i szkolnictwa wyższego	9
SUMA		371

Przyjęto następujące koszty utworzenia 1 stanowiska pracy:

Nazwa składnika	Koszt w zł
komputer osobisty (laptop)	7 500,00
stacja dokująca	800,00
telefon komórkowy	1 000,00
licencja MS Office	1 730,00
Suma:	11 030,00

Koszty te zostaną poniesione w 2025 r.

Utworzenie CSIRT sektorowych

Projekt ustawy przewiduje utworzenie zespołów CSIRT sektorowych, które będą wspierać podmioty kluczowe i podmioty ważne w reagowaniu na incydenty.

Koszty utworzenia i funkcjonowania CSIRT sektorowego będą różnić się od sektora (podsektora), dla którego realizuje zadania. Pod uwagę należy wziąć liczbę podmiotów w danym sektorze (podsektorze) oraz charakter świadczonych przez nich usług. Te czynniki będą determinowały jaki personel jest niezbędny w CSIRT sektorowym do realizacji zadań oraz jakie jest niezbędne oprogramowanie i sprzęt. To z kolei będzie miało wpływ na koszty funkcjonowania CSIRT sektorowych. Na potrzeby OSR przyjęto jako roczny koszt funkcjonowania CSIRT sektorowego kwotę 8 238 000,00 zł. Jest to kwota jaką wykazano w planie finansowym[10)] Centrum Cyberbezpieczeństwa w Zamościu, które

realizuje zadania publiczne polegające na ochronie publicznej cyberprzestrzeni, w szczególności cyberprzestrzeni resortu sprawiedliwości[11]. Należy tą kwotę traktować jako kwotę maksymalną.
Wydatki na utworzenie i funkcjonowanie CSIRT sektorowych zostaną poniesione z budżetu państwa, z poszczególnych części budżetowych organów właściwych do spraw cyberbezpieczeństwa. Jednakże w ramach Inwestycji C3.1.1 KPO *Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo* planowana jest realizacja projektu, pn. „utworzenie lub rozwój przynajmniej 5 sektorowych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT)". Przewidywana łączna wartość tego projektu wynosi ok. 66 000 000,00 zł netto. Planuje się, że w pierwszej kolejności utworzenie CSIRT sektorowych będzie w 2/3 sfinansowane ze środków KPO.
Przepisy nie określają formy prawnej podmiotu realizującego zadania CSIRT sektorowego, pozostawiając organowi właściwemu decyzję co do wyboru podmiotu, który stanie się takim CSIRT. Mogą to być zarówno jednostki budżetowe, jak i państwowe instytuty badawcze.
Planuje się, że zostaną utworzone następujące zespoły CSIRT sektorowe:

Część budżetowa	Nazwa części budżetowej	CSIRT sektorowy
20	Gospodarka	CSIRT produkcja, produkcja chemikaliów i przestrzeń kosmiczna
22	Gospodarka wodna	CSIRT woda pitna i ścieki
27	Informatyzacja	CSIRT infrastruktura cyfrowa/usługi cyfrowe/zarządzanie ICT
28	Szkolnictwo wyższe i nauka	CSIRT badania naukowe
32	Rolnictwo	CSIRT produkcja żywności
39	Transport	CSIRT transport
46	Zdrowie	CSIRT zdrowie, produkcja i urządzeń medycznych
47	Energia	CSIRT energia
51	Klimat	CSIRT gospodarowanie odpadami
76	Urząd Komunikacji Elektronicznej	CSIRT komunikacja elektroniczna i poczta

Dyrektywa NIS 2 określiła podmioty w ramach, których będą funkcjonować podmioty kluczowe i podmioty ważne. Sektory te są dla nas wiążące przy tworzeniu CSIRT sektorowych i na ich podstawie przygotowane zostało powyższe zestawienie. Nazwy CSIRT sektorowych ani ich dokładne zakresy nie są na obecnym etapie prac przesądzone. To na organach właściwych będzie spoczywał obowiązek ich organizacji. W przypadku gdy dwa lub więcej organów właściwych wyrazi zgodę możliwe będzie utworzenie jednego CSIRT sektorowego dla kilku sektorów. Powyższe zestawienie stanowi więc plan, który może ulegać zmianie. Przynależność sektora do poszczególnej części budżetowej ustalono na podstawie przepisów określających zakres poszczególnych działów administracji rządowej i funkcjonujących w nich organów.

Nie przewiduje się odrębnego CSIRT sektorowego dla podsektora transportu wodnego z uwagi na niewielką liczbę podmiotów w tym podsektorze. Zakłada się, że w ramach porozumienia dwóch organów do spraw cyberbezpieczeństwa podsektor ten będzie obsługiwany przez CSIRT transport.

CSIRT KNF będący obecnie sektorowym zespołem cyberbezpieczeństwa stanie się CSIRT sektorowym z dniem wejścia w życie ustawy i będzie otrzymywał dotację celową na swoje funkcjonowanie z cz. 16 budżetu państwa.
Centrum e-Zdrowie będący obecnie sektorowym zespołem cyberbezpieczeństwa stanie się CSIRT sektorowym z dniem wejścia w życie ustawy i będzie finansowane z części 46 budżetu państwa.

CSIRT NASK oraz CSIRT GOV będą pełnić funkcję CSIRT sektorowych dla podmiotów publicznych w zakresie dotychczasowego *constituency*. Pozwoli to na zachowanie ciągłości działań w tym obszarze oraz ułatwi podmiotom publicznym dostosowanie się do nowej sytuacji prawnej.

[10] Plan finansowy Centrum Cyberbezpieczeństwa zawiera załącznik nr 12 do ustawy budżetowej na rok 2024 z dnia 18 stycznia 2024 r. (Dz. U. poz. 122).

[11] § 2 ust. 1 zarządzenia Ministra Sprawiedliwości z dnia 8 października 2021 r. w sprawie utworzenia i nadania statutu instytucji gospodarki budżetowej pod nazwą „Centrum Cyberbezpieczeństwa Zamość" (Dz. Urz. Min. Sprawiedl. poz. 238).

	Urząd Dozoru Technicznego będzie pełnił rolę CSIRT sektorowego dla sektorów CSIRT produkcja, produkcja chemikaliów i przestrzeń kosmiczna. Zgodnie z proponowanymi przepisami UDT będzie finansował te zadania z własnego funduszu rezerwowego, co oznacza, że nie będzie potrzeby finansowania z budżetu państwa. Przyjęto kwotę 16 413,00 zł miesięcznego wynagrodzenia w CSIRT sektorowym (bez składek). Kwotę tę obliczono dzieląc kwotę 3 939 000,00 zł (wykazana w planie finansowym Centrum Cyberbezpieczeństwa jako kwotę wynagrodzeń osobowych) przez 20 zatrudnionych[12)] i 12 miesięcy. Przyjęto rocznie wzrost tej kwoty o 7,01%. Za planem finansowym Centrum Cyberbezpieczeństwa przyjęto per CSIRT w 2025 r.: 1) koszt usług obcych w wysokości 1 650 000,00 zł; 2) koszt materiałów i energii w wysokości 277 000,00 zł; 3) koszty amortyzacji w wysokości 280 000,00 zł; 4) pozostałe koszty funkcjonowania w wysokości 695 000,00 zł. W kolejnych latach doliczono do tych kosztów wzrost wskaźnika CPI w oparciu o *Wytyczne dotyczące stosowania jednolitych wskaźników makroekonomicznych będących podstawą oszacowania skutków finansowych projektowanych ustaw Aktualizacja – październik 2023 r*.[13)]. Zestawienie kosztów pojedynczego zespołu CSIRT sektorowego zawiera załącznik nr 2 do OSR. **Wzrost kwoty dotacji podmiotowej na CSIRT NASK** W związku z nowymi zadaniami zespołu CSIRT NASK przewiduje się zwiększenie kwoty dotacji podmiotowej na ten zespół. Zadanie będzie finansowane z części 27 budżetu państwa. Koszty przedstawiono w załączniku nr 3 do OSR. **Wzrost kwoty dotacji celowej na S46** System S46 utrzymywany i rozwijany jest przez Naukową i Akademicką Sieć Komputerową–Państwowy Instytut Badawczy będzie pełnił rolę wykazu podmiotów kluczowych i podmiotów ważnych, a także będzie podstawowym sposobem zgłaszania incydentów przez podmioty kluczowe i podmioty ważne. Stąd też konieczne jest zapewnienie odpowiedniego wzrostu dotacji celowej na rozwój tego systemu. Zadanie będzie finansowane z części 27 budżetu państwa. Koszty przedstawiono w załączniku nr 3 do OSR. Zwiększenie nakładów na utrzymanie i rozwój S46 jest związane z czynnikami wymienionymi poniżej: 1. Zwiększona o dwa rzędy wielkości liczba uczestników systemu S46 przekłada się na koszty obsługi systemu, zarówno jeśli chodzi o wsparcie oferowane przez poszczególne linie wsparcia, jak również w zakresie wsparcia merytorycznego. 2. Nowelizacja ustawy przewiduje uruchomienie rejestru podmiotów KSC zapewniającego podmiotom mechanizm samorejestracji za pośrednictwem sieci Internet i mechanizmów węzła krajowego. Uruchomienie bezpiecznego mechanizmu samorejestracji oraz wsparcie podmiotów podłączanych do S46 wymaga zwiększonych nakładów w stosunku do planowanych w obowiązującej ustawie. 3. W trakcie realizacji zadań związanych z utrzymaniem, okazało się konieczne powołanie zespołu analitycznego zdolnego do zauważania zależności, analizowania spójności modeli i ryzyk itp. W związku z nowelizacją powstanie większe zapotrzebowanie na tego rodzaju analizy. Należy wziąć pod uwagę również zatrudnienie specjalistów specjalizujących się w nowych technologiach, takich jak AI. Podniesienie nakładów umożliwi organizację zespołu analitycznego, który będzie mógł realizować funkcje wspomagające procesy analityczne zespołów CSIRT krajowych, zespołów CSIRT sektorowych oraz organów właściwych do spraw cyberbezpieczeństwa na poziomie systemu S46. 4. Doświadczenia dotyczące utrzymania i rozwoju systemu wskazują, że konieczne jest zapewnienie ciągłego doskonalenia funkcjonalności S46. Nowelizacja ustawy spowoduje wzrost liczby użytkowników co oznacza, że konieczne staje się utrzymanie stałego zespołu deweloperskiego, dedykowanego do ciągłego doskonalenia systemu, oraz wprowadzania poprawek. Zwiększenie liczby personelu dedykowanego do rozwoju systemu S46, umożliwi obsługę zwiększającej się skali i poziomu złożoności systemu. Brak dodatkowych nakładów w obszarze zespołów rozwojowych mógłby spowodować drastyczne wydłużenie okresu wprowadzania poprawek i dostosowywania

[12)] 20 osób zatrudnionych przyjęto za informacją dodatkową Centrum Cyberbezpieczeństwa do sprawozdania finansowego za 2022 r.

[13)] https://www.gov.pl/web/finanse/wytyczne-sytuacja-makroekonomiczna

systemu do wymagań zwiększonej w wyniku nowelizacji liczby użytkowników. Działania związane z utrzymaniem i rozwojem wymagają również inwestycji w narzędzia do analizy danych. Brak inwestycji w ww. narzędzia może wydłużyć czas reakcji na zagrożenia w obszarze cyberbezpieczeństwa.

Wsparcie kadrowe ministra właściwego do spraw informatyzacji w związku z nowymi zadaniami

Nowe zadania ministra właściwego do spraw informatyzacji w obszarze zarządzania kryzysowego w cyberprzestrzeni wymagają wsparcia kadrowego. Przewiduje się na to 4 etaty w urzędzie obsługującym ministra właściwego do spraw informatyzacji. Koszty zostaną poniesione z cz. 27 budżetu państwa.

Celem realizacji zadań w obszarze zarządzania kryzysowego niezbędny jest zakup sprzętu i oprogramowania umożliwiającego przetwarzanie informacji niejawnych.

1) zestaw komputerowy stacjonarny– stacja robocza + monitor + klawiatura + mysz + słuchawki – spełniający wymagania norm NATO serii SDIP- 27 LEVEL A – 4 szt.
2) drukarka laserowa A4 monochromatyczna – spełniająca wymagania norm NATO serii SDIP- 27 LEVEL A – 2 szt.
3) urządzenie wielofunkcyjne laserowe A4 kolor – spełniająca wymagania norm NATO serii SDIP-27 LEVEL A – 3 szt.
4) zewnętrzny moduł portów USB + czytnik kart 14 w 1 – spełniająca wymagania norm NATO serii SDIP- 27 LEVEL A – 6 szt.
5) słuchawki USB na złączu DB9 – spełniające wymagania norm NATO serii SDIP- 27 LEVEL A – 1 szt.
6) zasilacz awaryjny UPS – 4 szt.

Koszty tego sprzętu oszacowano na 489810,6 zł[14)]. Będzie to zakup jednorazowy w 2025 r. z części 27 budżetu państwa.

Aby zapewnić efektywność postępowań administracyjnych w sprawie uznania za dostawcę wysokiego ryzyka oraz postępowań w sprawach nałożenia administracyjnych kar pieniężnych za nie wycofanie produktów ICT, usług ICT i procesów ICT pochodzących od dostawcy wysokiego ryzyka przewiduje się wzmocnienie urzędu obsługującego ministra do spraw informatyzacji o 3 etaty. Zadanie będzie finansowane z części 27 budżetu państwa.

Powyższe 7 etatów przewiduje się od stycznia 2025 r. Kalkulacje przyjęto jak dla osób pełniących funkcje nadzorcze w organie właściwym do spraw cyberbezpieczeństwa.

Podnoszenie zdolności instytucji zapewniających cyberbezpieczeństwo

Przewiduje się możliwość, aby Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa mógł dokonywać zakupów sprzętu/oprogramowania dla uczestników posiedzeń Połączonego Centrum Operacyjnego Cyberbezpieczeństwa. Przewiduje się na to zadanie 50 619 520,00 zł rocznie począwszy od 2025 r.

Rodzaj	kwota
Endpoint Detection and Response (EDR) dla 10 000 podmiotów KSC	18 846 720,00
platforma CTI poziomu operacyjnego	18 920 000,00
platforma CTI z zakresu złośliwego oprogramowania dla 8 instytucji KSC	7 852 800,00
platforma CTI dla poziomu strategicznego	5 000 000,00
Suma	50 619 520,00

Zakup narzędzi Endpoint Detection & Response do 10 000 urządzeń końcowych – narzędzie służy do wykrywania podejrzanej aktywności na urządzeniach końcowych. Założono kwotę 40$ miesięcznie na jedno urządzenie końcowe. Przy 12 miesiącach i 10000 urządzeniach końcowych daję kwotę 18 846 720,00 zł[15].

Platforma CTI poziomu operacyjnego – platforma Cyber Threat Intelligence służąca do dostarczania i analizy w czasie rzeczywistym informacji o zagrożeniach w cyberprzestrzeni. Rozwiązanie wspiera organizacje w identyfikacji, ocenie i zarządzaniu ryzykiem związanym z cyberprzestępczością. Kwotę określono na podstawie zrealizowanego postępowania przetargowego na zakup dostępu do platformy

[14)] https://ezamowienia.gov.pl/mp-client/search/list/ocds-148610-64efbcf6-5d1a-11ee-9aa3-96d3b4440790

[15] Przy kursie dolara 3,9264 zł.

na rzecz 8 podmiotów Krajowego Systemu Cyberbezpieczeństwa. Numer ogłoszenia o zamówieniu lub o zamiarze zawarcia umowy Dz. Urz. UE: 2023/S 186-581359. Numer referencyjny postępowania: PN-17/C/2023.

Platforma CTI z zakresu złośliwego oprogramowania – platforma dla 8 podmiotów krajowego systemu cyberbezpieczeństwa (np. CSIRT sektorowych, CSIRT poziomu krajowego, służb specjalnych) służąca do dostarczania i analizy informacji o złośliwym oprogramowaniu. Założono kwotę 250 000 $ rocznie per podmiot co przy kursie $ 3,9264 daje łącznie 7 852 800,00 zł.

Platforma CTI poziomu strategicznego – Platforma/System służąca do dostarczania informacji z zakresu Cyber Threat Intelligence o poziomie strategicznym na rzecz podmiotów zapewniających bezpieczeństwo teleinformatyczne w ramach funkcjonowania Krajowego Systemu Cyberbezpieczeństwa. Dostarcza dane o zagrożeniach w cyberprzestrzeni za pomocą algorytmów lub programów typu crawler i dedykowanych zespołów analityków cyberbezpieczeństwa (zespół minimalnie 200 osób, praca w reżimie 24/7/365) przynajmniej z otwartych oraz zamkniętych źródeł. Kwota zamówienia określona na podstawie szacowania rynkowego.

Działalność edukacyjna
Przewiduje się także zapewnienie środków na działalność edukacyjną ministra właściwego do spraw informatyzacji. Działalność ta polega na wspieraniu świadomości co do cyberzagrożeń. Przewidziano na to zadanie 12 630 000,00 zł rocznie od 2025 r. Będą to programy edukacyjne, szkolenia z zakresu cyberbezpieczeństwa, a także zakupy usług i oprogramowania wspierające te programy, np. platformy szkoleniowe. Koszty Programów opracowano na podstawie dotychczasowych działań Ministra Cyfryzacji – programów SecureV, Bezpieczni w Sieci i CyberLekcji.

Badania/ekspertyzy na rzecz Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa
Projekt ustawy przewiduje możliwość zlecenia przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa badań, które mają na celu wsparcie realizacji jego zadań. Przewiduje się na to zadanie 100 000,00 zł rocznie począwszy od 2025 r.

Koszt zakupu licencji do norm technicznych i innych dokumentów standaryzacyjnych z zakresu Cyberbezpieczeństwa
Aby wykonywać czynności nadzorcze organ właściwy do spraw cyberbezpieczeństwa musi mieć dostęp do niezbędnej wiedzy. W tym celu zasadne jest, aby rokrocznie organy mogły zakupić normy techniczne i inne dokumenty normalizacyjne z zakresu cyberbezpieczeństwa. Przewiduje się że w 2025 r. koszt wyniesie 7 000 zł per organ właściwy do spraw Cyberbezpieczeństwa, a od 2026 r. 8 000 zł.

Badanie sprzętu lub oprogramowania
Przewiduje się rocznie 3 mln zł dla Agencji Bezpieczeństwa Wewnętrznego na prowadzenie badań sprzętu lub oprogramowania pod kątem identyfikacji podatności zagrażającej bezpieczeństwu narodowemu.

Wpływ finansowy projektu na podmioty publiczne
Podmioty publiczne w tym jednostki samorządu terytorialnego już obecnie są obowiązane do zgłaszania incydentów w podmiocie publicznym oraz do zarządzania incydentami, co wynika z art. 22 KSC. Ponadto podmioty publiczne mają obowiązek wdrożenia systemu zarządzania bezpieczeństwem informacji i przeprowadzania m.in. audytów (co wynika z § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz. U. z 2017 r. poz. 2247). Podsumowując już obecnie jednostki samorządu terytorialnego mają obowiązki z zakresu cyberbezpieczeństwa i na to powinny mieć przeznaczone środki finansowe w budżecie. Dostosowanie się podmiotów publicznych, w tym jednostek samorządu terytorialnego, do wymogów dyrektywy NIS2 będzie polegało na przeglądzie już wdrożonych systemów zarządzania bezpieczeństwem informacji i uzupełnienia dokumentacji oraz środków technicznych i organizacyjnych. Skala zmian będzie zależna od obecnej dojrzałości organizacyjnej poszczególnych podmiotów publicznych. Oszacowanie kosztów dostosowawczych nie jest możliwe.
W ramach Inwestycji C3.1.1. KPO *Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo* przewiduje się m.in. realizację projektu pn. „*Wsparcie 500 podmiotów krajowego systemu*

	cyberbezpieczeństwa w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT, w tym wsparcie podmiotów wykorzystujących technologie informacyjne (IT) oraz operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS)". Projekt ten zakłada udzielenie wsparcia o wartości – ok. 700,5 mln zł m.in. dla ok. 70 urzędów administracji centralnej i rządowej W ramach tego projektu urzędy administracji centralnej i rządowej będą mogły uzyskać wsparcie finansowe na dostosowanie się do projektowanej ustawy. Ponad 2 500 samorządów (blisko 90%) otrzyma w bieżącym roku wsparcie finansowe w postaci grantów finansowanych ze środków budżetu państwa oraz programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa. Wsparcie to jednostki samorządu terytorialnego będą mogły wykorzystać na modernizację rozwiązań w obszarze cyberbezpieczeństwa. Łączna wartość wsparcia jaka zostanie przekazana wyniesie ok. 1,5 mld zł.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

Skutki								
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							
	(dodaj/usuń)							
W ujęciu niepieniężnym	duże przedsiębiorstwa	Celem dostosowania się do wymogów projektu przedsiębiorstwa będą musiały wdrożyć środki techniczne i organizacyjne proporcjonalne do wielkości podmiotu. W przypadku dużych przedsiębiorstw może to zająć pewien czas. Niezbędne będzie dokonanie inwentaryzacji infrastruktury, przeglądu procesów i wewnętrznych procedur, przeprowadzenie wewnętrznych szkoleń. Każdy z podmiotów będzie musiał zbudować system zarządzania bezpieczeństwem uwzględniający kwestie takie jak np. 1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem; 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, w szczególności utrzymanie i bezpieczną eksploatację systemu informacyjnego; 3) zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi; 4) zarządzanie incydentami; 5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi. Dyrektywa NIS 2 odeszła od wprowadzania konkretnych wymogów bezpieczeństwa na rzecz podejścia opartego na ryzyku. W związku z tym każdy podmiot objęty jej postanowieniami musi sam przeprowadzić analizę ryzyka oraz dostosować stosowane zabezpieczenia do wykrytego ryzyka. Takie rozwiązanie zapewnia elastyczność jak również proporcjonalność wprowadzanych zabezpieczeń do charakteru danej organizacji.						

		Na tym etapie nie jest możliwe oszacowanie kosztów dostosowawczych po stronie przedsiębiorców w zależności od ich rodzajów z uwagi na brak danych. Projekt oddziałuje na podmioty o zróżnicowanej wielkości – od małych do dużych. Koszty audytów bezpieczeństwa, zatrudnienia specjalistów z zakresu cyberbezpieczeństwa, wdrożenia systemu zarządzania bezpieczeństwem informacji itd., będą się znacząco różnić od wielkości i charakteru usług świadczonych przez podmiot. Zasadne będzie poniesienie kosztów na sprzęt, oprogramowanie oraz zatrudnienie nowego personelu. Konieczny może być zakup zewnętrznych usług konsultingowych z zakresu cyberbezpieczeństwa. Warto zauważyć, że już obecnie duże przedsiębiorstwa mają działy zajmujące się cyberbezpieczeństwem, co powinno im ułatwić dostosowanie się do projektu ustawy. Należy zauważyć, że wymogi te stosowane będą jednolicie w całej Unii Europejskiej w związku z czym nie powinno dojść do zaburzeń konkurencyjności. Sama ustawa przewiduje jednakowe dla wszystkich podmiotów kluczowych. Również wymogi dla pomiotów ważnych nie będą różnicowane. Podmioty krajowego systemu cyberbezpieczeństwa będą obowiązane wycofać produkty ICT, usługi ICT i procesy ICT dostawcy uznanego za dostawcę wysokiego ryzyka. Będzie to generowało koszty związane z wycofaniem tego tych produktów, usług i procesów oraz zastąpienie innymi. W tym momencie nie jest jednak możliwe oszacowanie tych kosztów.
	sektor mikro-, małych i średnich przedsiębiorstw	Projekt ma wpływ na co najmniej średnie przedsiębiorstwa, z wyjątkami takimi jak przedsiębiorcy komunikacji elektronicznej czy dostawcy usług zaufania – ci będą podlegać ustawie niezależnie od wielkości. Projekt przewiduje, że podmioty kluczowe i podmioty ważne będą wdrażać środki techniczne i organizacyjne proporcjonalne do wielkości podmiotu – uwzględniona została więc sytuacja podmiotów z sektora MŚP. Na tym etapie nie jest możliwe oszacowanie kosztów dostosowawczych po stronie przedsiębiorców w zależności od ich rodzajów z uwagi na brak danych. Projekt oddziałuje na podmioty o zróżnicowanej wielkości – od małych do dużych. Koszty audytów bezpieczeństwa, zatrudnienia specjalistów z zakresu cyberbezpieczeństwa, wdrożenia systemu zarządzania bezpieczeństwem informacji itd., będą się znacząco różnić od wielkości i charakteru usług świadczonych przez podmiot. Projekt może być uzupełniony w tym zakresie, jeżeli w toku konsultacji publicznych zostaną przedstawione dane dotyczące kosztów wdrożenia. Podmioty krajowego systemu cyberbezpieczeństwa będą obowiązane wycofać produkty ICT, usługi ICT i procesy ICT dostawcy uznanego za dostawcę wysokiego ryzyka. Będzie to generowało koszty związane z wycofaniem tego tych produktów, usług i procesów oraz zastąpienie innymi. W tym momencie nie jest jednak możliwe oszacowanie tych kosztów.
	rodzina, obywatele oraz gospodarstwa domowe	Rodziny, obywatele, gospodarstwa domowe – regulacje ustawowe przyczynią się do zwiększenia bezpieczeństwa usług, z których korzystają wszyscy obywatele. Zwiększą pewność ciągłości usług. Polepszy się ochrona danych osobowych przetwarzanych przez podmioty ważne i podmioty kluczowe. Kierownik podmiotu kluczowego lub podmiotu ważnego będzie podlegał odpowiedzialności karno-administracyjnej za

		niewykonywanie zadań z zakresu cyberbezpieczeństwa w podmiocie. Tylko osoby niekarane za przestępstwa przeciwko ochronie informacji będą mogły realizować w podmiocie kluczowym lub podmiocie ważnym zadania związane z zarządzaniem ryzykiem cyberbezpieczeństwa oraz obsługi i zgłaszania incydentów. Organy właściwe do spraw cyberbezpieczeństwa, zespoły CSIRT sektorowe, zespoły CSIRT poziomu krajowego i minister właściwy do spraw informatyzacji będą przetwarzały dane osobowe osób do kontaktu wskazanych przez podmioty kluczowe i podmioty ważne. Odbywać to się będzie z zachowaniem właściwości poszczególnych organów czy zespołów. Dane te będą znajdowały się w wykazie podmiotów kluczowych i podmiotów ważnych. Dane te nie będą dostępne publicznie. Obecnie istnieje podobny obowiązek wskazania po 1 osobie do kontaktu przez podmioty publiczne i operatorów usług kluczowych.
Niemierzalne	Koszty związane z wycofaniem sprzętu lub oprogramowania od dostawców wysokiego ryzyka	Nowelizacja przewiduje kompetencję dla ministra właściwego do spraw informatyzacji do wydania decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Nie jest możliwe w tej chwili wskazanie kosztów jakie poniosą podmioty kluczowe i podmioty ważne w związku z wycofaniem produktów ICT, usług ICT i procesów ICT pochodzących od dostawców wysokiego ryzyka, ponieważ nie można w tej chwili przewidzieć jaką decyzję wyda minister właściwy do spraw informatyzacji i w związku z tym jakie koszty poniosą podmioty zobowiązane do wycofania sprzętu. Należy podkreślić, że w zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty kluczowe i podmioty ważne zostaną zobowiązane do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 5–7 latach – termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla przedsiębiorców z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka.
	Koszty związane z wykonaniem polecenia zabezpieczającego	Nowelizacja przewiduje nowe kompetencje dla ministra właściwego do spraw informatyzacji do wydania polecenia zabezpieczającego w drodze decyzji administracyjnej. Nie jest możliwe w tej chwili wskazanie kosztów jakie poniosą podmioty krajowego systemu cyberbezpieczeństwa, ponieważ polecenie zabezpieczające będzie wydawane po wystąpieniu incydentu krytycznego. Podkreślić przy tym należy, że polecenie zabezpieczające ma być adekwatne do cyberzagrożenia.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Wpływ na konkurencyjność gospodarki i przedsiębiorczość będzie różnił się w zależności od typu podmiotu i sektora. Nie jest możliwe oszacowanie kosztów dostosowania się przedsiębiorców do wymogów określonych w nowelizacji. Wynika to z faktu, że konkretne środki techniczne i organizacyjne stosowane przez przedsiębiorców będą zależne od przeprowadzonego szacowania ryzyka. Innego rodzaju środki będą stosować operatorzy zarządzający własną infrastrukturą telekomunikacyjną, a inne dostawcy usług komunikacji elektronicznej, którzy swoją działalność opierają o infrastrukturę innego operatora. Ponadto nie są znane konkretne środki już teraz stosowane przez przedsiębiorców – często, z powodów bezpieczeństwa, informacja o tych środkach stanowi tajemnicę przedsiębiorstwa.	

	Podkreślić należy, że nakładane obowiązki z zakresu zarządzania ryzykiem cyberbezpieczeństwa pokrywają się z normami technicznymi i innymi standardami stosowanymi dobrowolnie przez przedsiębiorców. Wielu przedsiębiorców już teraz wdraża systemy zarządzania bezpieczeństwem informacji zgodne z normą ISO 27001 oraz systemy zarządzania ciągłością działania zgodne z normą ISO 22301. Część z tych przedsiębiorców uzyskuje nawet certyfikację zgodności z tymi normami. Nie są to oczywiście jedyne sposoby zapewnienia zgodności z projektowanymi przepisami. Niemniej część obowiązków proponowanych w projekcie jest już obecnie stosowana przez przedsiębiorców. Zakłada się, że nowo powstałe zespoły CSIRT sektorowe będą aktywnie wspierać przedsiębiorców w reagowaniu na incydenty, ale także w przekazywaniu informacji o cyberzagrożeniach i podatnościach. CSIRT sektorowe będą także prowadzić działalność szkoleniową. Ideałem jest osiągnięcie wzajemnego zaufania między podmiotami kluczowymi i podmiotami ważnymi z danego sektora a CSIRT sektorowym. Projekt nakłada jedynie konieczne i niezbędne obowiązki, aby osiągnąć cele ustawy. Projekt nie wprowadza regulacji dot. zakazu wykonywania określonej działalności gospodarczej. Z tych powodów uznaje się, że projekt jest zgodny z ustawą z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2024 r. poz. 236, z późn. zm.). Projekt zakłada przetwarzanie danych osobowych w minimalnym zakresie – niezbędnym do realizacji czynności nadzorczych organów właściwych do spraw cyberbezpieczeństwa, realizacji zadań zespołów CSIRT w zakresie reagowania na incydenty czy wykonywania obowiązków wynikających z prawa unijnego.

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☒ tak ☐ nie ☐ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☒ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy

Komentarz:

Nałożono obowiązki na podmioty kluczowe i podmioty ważne zgodne z wykazem tych podmiotów wskazanych w załączniku nr 1 i 2 do dyrektywy NIS2. Będą one obowiązane dokonać samorejestracji w wykazie podmiotów kluczowych i ważnych, co umożliwi ich identyfikację, aktywne wsparcie ich przez zespoły CSIRT sektorowe i zespoły CSIRT poziomu krajowego oraz wykonywanie czynności nadzorczych przez organy właściwe do spraw cyberbezpieczeństwa. Umożliwi to także przekazywanie danych o liczbie tych podmiotów do Komisji Europejskiej i Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa.

Podmioty kluczowe i podmioty ważne będą obowiązane wprowadzić system zarządzania bezpieczeństwem informacji w procesach służących świadczeniu usług przez te podmioty. Odpowiada to zakresowi wymogów co do środków zarządzania ryzykiem wskazanych w art. 21 dyrektywy NIS 2.

Kierownik podmiotu kluczowego lub podmiotu ważnego będzie odpowiedzialny za realizację tych zadań przez podmiot – i będą mogły być nałożone na niego kary. Będzie miał też obowiązek przejścia stosownego szkolenia z zakresu cyberbezpieczeństwa.

Tak jak do tej pory operatorzy usług kluczowych tak i inne podmioty kluczowe będą obowiązane przeprowadzać audyty bezpieczeństwa swoich systemów informacyjnych. Audyty będą przeprowadzane co trzy lata. W przypadku

podmiotów ważnych audyt będzie przeprowadzany na podstawie decyzji organu właściwego do spraw Cyberbezpieczeństwa.

Projektowana ustawa w zakresie zgłaszania incydentów zwiększa liczbę obowiązków nakładanych na podmioty objęte jej regulacją. Podmioty kluczowe i ważne będą w pierwszej kolejności zgłaszać wczesne ostrzeżenie o incydencie poważnym. Zgłoszenia będą kierowane do CSIRT sektorowego. Wczesne ostrzeżenie będzie mogło zawierać wniosek o wskazanie wytycznych dotyczących możliwych do wdrożenia środków ograniczających skutki incydentu poważnego lub o wsparcie techniczne przy obsłudze incydentu. Po otrzymaniu takiego wniosku CSIRT sektorowy zobowiązany będzie do udzielenia stosownego wsparcia podmiotowi zgłaszającemu taki wniosek. Następnie dokonywane będzie zgłoszenie incydentu. W trakcie obsługi incydentu, na wniosek właściwego CSIRT sektorowego, przekazywane będzie sprawozdanie okresowe, a po zakończeniu obsługi incydentu – sprawozdanie końcowe.

CSIRT sektorowe będą przedstawiały Pełnomocnikowi Rządu do Spraw Cyberbezpieczeństwa sprawozdanie z działalności za poprzedni rok.

Podmioty, które mogą spełniać kryteria uznania za podmioty kluczowe lub podmioty ważne będą mogły być „odpytywane" przez organy właściwe do spraw cyberbezpieczeństwa o informacje, które pozwolą ustalić ich status. Brak udzielenia odpowiedzi będzie skutkował nałożeniem administracyjnej kary pieniężnej.

Nowym zadaniem ministra właściwego do spraw informatyzacji będzie przygotowanie Krajowego Planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę. Dokument ten będzie określał zasady postępowania w przypadku wystąpienia takiego incydentu oraz zasady współpracy między organami realizującymi zadania z zakresu cyberbezpieczeństwa oraz organami właściwymi do spraw zarządzania kryzysowego. i będzie przyjmowany w drodze uchwały Rady Ministrów. Minister właściwy do spraw informatyzacji będzie również prosił o wkłady inne organy, zwłaszcza te działające w obszarze zarządzania kryzysowego.

Minister właściwy do spraw informatyzacji będzie również dalej realizował zadania pojedynczego punktu kontaktowego oraz przygotowywał i aktualizował krajową strategię cyberbezpieczeństwa. Dalej będzie również działał w ciałach kolegialnych Unii Europejskiej zajmujących się cyberbezpieczeństwem.

CSIRT NASK będzie pełnił rolę koordynatora na potrzeby skoordynowanego ujawniania podatności. W związku z powyższym konieczne będzie przygotowanie procedur w tym zakresie, w szczególności w obszarze komunikacji z producentami sprzętu i oprogramowania, u których będą wykrywane podatności.

Projektowane przepisy przewidują również udział polskich organów ds. cyberbezpieczeństwa w procedurze wzajemnej oceny z organami z innych krajów Unii Europejskiej. Wymaga to przygotowania procedur związanych z ich wyjazdami zagranicznymi oraz przyjmowaniem przedstawicieli innych państw w Polsce.

W związku z nałożeniem na podmioty krajowego systemu cyberbezpieczeństwa szeregu obowiązków istotne zmiany zachodzą w przepisach dotyczących nadzoru i egzekwowania przepisów, a także nakładania kar administracyjnych. Projektowane regulacje wyposażają organy właściwe do spraw cyberbezpieczeństwa w szerokie kompetencje nadzoru i egzekwowania przepisów takie jak wydawanie ostrzeżeń, nakazów, decyzji administracyjnych nakazujących podjęcie lub zaniechanie określonego działania. Organy te zostaną również wyposażone w środki, które znajdą zastosowanie w sytuacji, w której podmiot kluczowy lub podmiot ważny nie wykonał w terminie postanowień określonych w ostrzeżeniu, nakazie czy decyzji. Wśród obowiązków nakładanych na organy właściwe do spraw cyberbezpieczeństwa należy wymienić w szczególności obowiązek brania pod uwagę określonych kryteriów, które należy przeanalizować w celu podjęcia działań nadzorczych i egzekwowania przepisów, a także wymierzając karę pieniężną.

Rozbudowany został również katalog przypadków określających kiedy podmioty kluczowe lub podmioty ważne podlegają karze pieniężnej. Oznacza to co do zasady zwiększenie zadań dla organów właściwych do spraw cyberbezpieczeństwa, które będą musiały nakładać kary pieniężne za określone działania lub zaniechania, których dopuszczać się będą podmioty kluczowe lub podmioty ważne. Ponownie należy podkreślić, że wymierzając karę pieniężną organy właściwe do spraw cyberbezpieczeństwa obligatoryjnie będą musiały dokonywać analizy określonych w projektowanych przepisach przesłanek.

9. Wpływ na rynek pracy

Nowe regulacje w związku z objęciem wielu nowych podmiotów obowiązkami zwiększą zapotrzebowanie na usługi i ekspertów z zakresu cyberbezpieczeństwa. Wpłyną również pozytywnie na firmy świadczące usługi z tego zakresu, które mogą liczyć na zwiększenie popytu na ich usługi. W związku z tym należy spodziewać się, że aby poradzić sobie z tym wzrostem zapotrzebowania będą one musiały zatrudnić dodatkowe osoby.

Należy podkreślić, że większy nacisk jaki będzie kładziony na cyberbezpieczeństwo może wpłynąć pozytywnie również na inne zawody związane z informatyką. Dyrektywa NIS 2 promuje podejście „security by design", które zakłada uwzględnienie wymagań bezpieczeństwa już na etapie projektowania rozwiązań informatycznych. Tworzenie

takich rozwiązań oraz większa dbałość o bezpieczeństwie systemów w ramach codziennej działalności również będzie wymagało dodatkowych osób.

Projekt zwiększy zapotrzebowanie na specjalistów z zakresu cyberbezpieczeństwa – operatorów 1, 2, 3 linii operacyjnego centrum bezpieczeństwa, analityków cyberzagrożeń, podatności, specjalistów ds. świadomości cyberbezpieczeństwa (awareness), menedżerów z zakresu cyberbezpieczeństwa. Ponadto będzie zapotrzebowanie na audytorów przeprowadzających audyty bezpieczeństwa.

Z powyższych względów wpływ projektu na rynek pracy należy uznać za pozytywny.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne	☐ demografia	☒ informatyzacja
☐ sytuacja i rozwój regionalny	☐ mienie państwowe	☐ zdrowie
☒ sądy powszechne, administracyjne lub wojskowe	☐ inne:	

Omówienie wpływu	Znaczne zwiększenie nacisku na cyberbezpieczeństwo będzie miało pozytywny wpływ na informatyzację. Nowe wymogi sprawią, że wzrośnie znaczenie rynkowe produktów, które zapewniają odpowiedni poziom cyberbezpieczeństwa. Wzrost popytu na takie rozwiązania będzie powodował, że producenci będą musieli dostarczyć produkty i usługi dostosowane do klientów. Przy projektowaniu i tworzeniu tych produktów będą brane pod uwagę kwestie cyberbezpieczeństwa. Będzie to miało pozytywny wpływ na cały rynek ICT, gdyż zwiększy dostępność bezpiecznych rozwiązań ICT. Projekt ustawy przewiduje nowe administracyjne kary pieniężne. Skargi na decyzje administracyjne w sprawie nałożenia kary będą rozpatrywały sądy administracyjne. Utworzony zostanie nowy wykaz – wykaz podmiotów kluczowych i podmiotów ważnych. Za jego funkcjonowanie będzie odpowiedzialny minister właściwy do spraw informatyzacji. Przewiduje się powierzenie realizacji tego zadania Naukowej i Akademickiej Sieci Komputerowej–Państwowemu Instytutowi Badawczemu, z uwagi na to, że wykaz będzie funkcjonował w systemie S46, który już obecnie jest prowadzony przez NASK–PIB.

11.Planowane wykonanie przepisów aktu prawnego

Projektowana ustawa wejdzie w życie w terminie miesiąca od dnia ogłoszenia.

Pierwszym krokiem będzie utworzenie przez ministra właściwego do spraw informatyzacji wykazu podmiotów kluczowych i podmiotów ważnych. Podmioty, które w dniu wejścia w życie projektowanej ustawy spełniają kryteria dla podmiotu kluczowego i podmiotu ważnego będą obowiązane zarejestrować się w wykazie. Minister właściwy do spraw informatyzacji udostępni w Biuletynie Informacji Publicznej harmonogram rejestracji, aby przeciwdziałać obciążeniu systemu.

Podmioty kluczowe i podmioty ważne otrzymają 6 miesięcy okresu dostosowawczego do nowych obowiązków.

W zakresie utworzenia CSIRT sektorowych pierwszym krokiem będzie zaplanowanie budowy takiej instytucji – wybranie podmiotu, który będzie realizował to zadanie, zaplanowanie budżetu, określenie liczby etatów, zaplanowanie struktury zespołu. Następnie konieczne będzie zapewnienie lokalizacji, sprzętu, oprogramowania, rekrutacja kadr. Po uzyskaniu zdolności operacyjnej nastąpi ogłoszenie tej informacji w dzienniku urzędowym organu właściwego do spraw cyberbezpieczeństwa – od tego momentu podmioty kluczowe/ podmioty ważne będą zgłaszać incydenty do danego CSIRT sektorowego. Niezależnie od tego powinna być przeprowadzona akcja informacyjna w ramach sektora – spotkania, konferencje mające przybliżyć zespół CSIRT, a także budować zaufanie między podmiotami a zespołem.

Polecenie zabezpieczające oraz postępowanie w sprawie uznania za dostawcę wysokiego ryzyka będą stosowane w razie zaistnienia potrzeby.

12. w jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Zastosowane będą następujące mierniki:

1) liczba podmiotów wpisanych do wykazu podmiotów kluczowych i podmiotów ważnych;
2) liczba zgłoszonych incydentów poważnych w danym roku kalendarzowym;
3) liczba przeprowadzonych audytów przez podmioty kluczowe;
4) liczba incydentów krytycznych w danym roku kalendarzowym;
5) liczba nałożonych administracyjnych kar pieniężnych.

Mierniki te dadzą odpowiedź na pytanie, czy i w jaki sposób przepisy ustawy są stosowane. Zostanie też przeprowadzona analiza orzecznictwa sądów w sprawach dot. odpowiedzialności administracyjnej wynikającej z nowych przepisów. Analiza ta wykaże istotne kwestie w wykładni przepisów ustawy przez sądy. Będzie ona stanowiła podstawę do ustalenia, czy konieczna jest interwencja prawodawcy celem doprecyzowania przepisów ustawy.

Dzięki obowiązkowi sprawozdawania się przez CSIRT sektorowe Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa będzie w stanie dokonać oceny ich funkcjonowania, w ramach jego kompetencji do oceny funkcjonowania krajowego systemu cyberbezpieczeństwa, w szczególności wzięte pod uwagę zostaną takie kwestie jak: liczba zgłoszonych incydentów do danego CSIRT, w tym liczba zgłoszonych incydentów poważnych, czas reagowania na incydenty, a także pozostała działalność CSIRT sektorowego, liczba przeprowadzonych działań edukacyjnych wśród podmiotów kluczowych/ podmiotów ważnych.

Monitorowana będzie liczba incydentów poważnych, a także przyczyny ich wystąpienia.

Ewaluacja nastąpi dwa lata po wejściu ustawy w życie, a następnie będzie prowadzona cyklicznie, co dwa lata.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Załącznik nr 1 do OSR – Dostawca wysokiego ryzyka (high risk vendor) i bezpieczeństwo sieci 5G w Europie;

Załącznik nr 2 do OSR – Koszty pojedynczego zespołu CSIRT sektorowego w zł;

Załącznik nr 3 do OSR – Ocena skutków regulacji KSC 2.0 dla NASK-PIB w latach 2025–2034

Estymacja kosztów;

Załącznik nr 4 do OSR – podsumowanie wydatków dla poszczególnych części budżetowych w zł.