Nazwa projektu Projekt ustawy o krajowym systemie cyberbezpieczeństwa **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Krzysztof Silicki, Podsekretarz Stanu w Ministerstwie Cyfryzacji **Kontakt do opiekuna merytorycznego projektu** Andrzej Szyszko, Departament Cyberbezpieczeństwa, Naczelnik Wydziału Strategii i Współpracy Międzynarodowej, tel. (22) 245 57 05, e-mail: andrzej.szyszko@mc.gov.pl	**Data sporządzenia** 27 października 2017 **Źródło:** Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1). **Nr w wykazie prac legislacyjnych Rady Ministrów** UD31

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Współcześnie rozwój społeczny i gospodarczy w znacznym stopniu zależny jest od szybkiego i nieskrępowanego dostępu do informacji. Obecność technologii teleinformatycznych, w tym operacje na dużych zasobach danych, służą świadczeniu szerokiej gamy usług, mających kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, w tym m.in. usług finansowych, transportowych, z zakresu ochrony zdrowia, energii, zaopatrzenia w wodę pitną. Każde znaczące zakłócenie funkcjonowania cyberprzestrzeni będzie miało również wpływ na poczucie bezpieczeństwa obywateli, sprawność funkcjonowania instytucji sektora publicznego a także świadczenie usług przez przedsiębiorców, a w rezultacie również na ogólnie pojmowane bezpieczeństwo państwa. W związku z tym niezbędne jest wprowadzenie rozwiązań pozwalających na stworzenie skutecznego i efektywnego systemu bieżącego monitorowania oraz zarządzania cyberbezpieczeństwem w skali kraju.

Projektowana ustawa stanowi implementację dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, zwanej dalej „dyrektywą 2016/1148/UE". Ponadto, wpisuje się w cel 5 Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022 – Osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów informacyjnych istotnych dla funkcjonowania państwa.

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

Celem ustawy jest w szczególności:

1) organizacja oraz określenie sposobu funkcjonowania krajowego systemu cyberbezpieczeństwa, w tym:
   a) wskazanie sektorów gospodarki narodowej, dla których zastosowanie będą miały przepisy ustawy oraz określenie kryteriów kwalifikacji podmiotów objętych regulacją, a więc operatorów usług kluczowych;
   b) określenie minimalnych wymagań bezpieczeństwa teleinformatycznego dla systemów informacyjnych operatorów usług kluczowych i dostawców usług cyfrowych;
   c) przedstawienie rozwiązań systemowych i struktur zajmujących się cyberbezpieczeństwem na poziomie regulacyjnym, koordynacyjnym i technicznym;
   d) ustalenie ustawowych wymagań i powinności z zakresu cyberbezpieczeństwa dla zespołów reagowania na incydenty bezpieczeństwa komputerowego;
2) określenie sposobu sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy,
3) prawne umocowanie dokumentu ustanawiającego krajową Strategię Cyberbezpieczeństwa Rzeczpospolitej Polskiej;

Efektem wprowadzonej regulacji będzie podniesienie odporności usług kluczowych świadczonych z wykorzystaniem technologii informatycznych na ataki pochodzące z cyberprzestrzeni. Tym samym projektowana regulacja przyczyni się do lepszego zapewnienia ciągłości działania tych usług tak, aby zarówno obywatele jak i przedsiębiorstwa miały do nich stały i niezakłócony dostęp.

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

Dyrektywa 2016/1148 jest w trakcie transpozycji w innych państwach członkowskich UE, jednakże w wielu z nich wprowadzono w ostatnich miesiącach albo jeszcze przed wejściem w życie dyrektywy różnorodne rozwiązania prawne i organizacyjne w zakresie zapewnienia cyberbezpieczeństwa, których część została opisana poniżej.

Wielka Brytania:

W lutym 2017 r. w Wielkiej Brytanii została zainagurowana działalność Narodowego Centrum Cyberbezpieczeństwa (National Cyber Security Centre – NCSC). Zadaniem Centrum jest pomoc administracji publicznej i przedsiębiorstwom w reagowaniu na poważne incydenty w dziedzinie cyberbezpieczeństwa oraz zwiększenie bezpieczeństwa w Internecie, dzięki działalności doradczej oraz pomocy technicznej. Przykładowe działania obejmują przeszukiwanie luk w zabezpieczeniach stron internetowych sektora publicznego, czy blokowanie fałszywych maili celem zapobiegania atakom phishingowym.

NCSC, organizacyjnie, jest częścią brytyjskiej agencji wywiadu i bezpieczeństwa (Government Communications Headquarters – GCHQ). Zostało powołane w celu implementacji dyrektywy 2016/1148 i pełni rolę punktu kontaktowego. Koszty uruchomienia i funkcjonowania NCSC do 2020 r., w tym koszty organizacyjne i zatrudnienia 100 najlepszych specjalistów z zakresu cyberbezpieczeństwa, którzy wcześniej pracowali w prywatnych przedsiębiorstwach to 1,9 mld funtów.

Powołanie NCSC jest kolejnym etapem rozbudowy systemu cyberbezpieczeństwa w Wielkiej Brytanii. Do tej pory kluczową instytucją w systemie był CERT-UK liczący około 55 pracowników i realizujący typowe zadania dla CERT/CSIRT, czyli zarządzanie krajowymi incydentami z zakresu cyberbezpieczeństwa, w tym wsparcie dla podmiotów dotkniętych incydentem oraz promowanie świadomości dotyczącej zagrożeń w cyberprzestrzeni. Funkcjonują również partnerstwa publiczno-prywatne, polegające na wymianie informacji na temat zagrożeń i luk bezpieczeństwa w systemach teleinformatycznych (Cyber-security Information Sharing Partnership – inicjatywa CERT-UK) oraz mniejsze, kilkunastoosobowe zespoły analityczne jak np. Fusion Cell złożony z przedstawicieli rządu i służb państwowych (pracowników m.in. GCHQ, MI5, MI6 i Policji). Biorąc pod uwagę system prawa w Wielkiej Brytanii rolą NCSC jest zachęcanie organizacji do zarządzania własnym ryzykiem w zakresie cyberbezpieczeństwa. Centrum wydaje rekomendacje, wytyczne i zapewnia wsparcie dotyczące cyberbezpieczeństwa, w tym w zakresie zarządzania incydentami.

Holandia:

Narodowe Centrum Cyberbezpieczeństwa (NCSC)[1], jest od 2012 r. głównym podmiotem odpowiedzialnym za zapewnienie bezpieczeństwa cyberprzestrzeni w Holandii i podlega Ministerstwu Bezpieczeństwa i Sprawiedliwości. NCSC samodzielnie lub na wniosek wydaje wytyczne i rekomendacje urzędom administracji publicznej i operatorom sektorów krytycznych w związku z najważniejszymi ujawnionymi podatnościami i w sytuacji poważnych zdarzeń kryzysowych w dziedzinie cyberbezpieczeństwa. Centrum dysponuje sieciami typu „honey-pot" dla administracji centralnej i sektorów krytycznych (projekty sieci były zbudowane w kooperacji z polskim NASK). W jego strukturze znajduje się m.in. narodowy/rządowy CERT, uczestniczący w sieci European Governmental CERTs (EGC). W związku z rewizją strategii cyberbezpieczeństwa, przyjętą w 2013 r. kompetencje NCSC zostały poszerzone o struktury odpowiedzialne za wymianę i analizę informacji niejawnych. Ponadto dodano kompetencje w zakresie monitorowania w czasie rzeczywistym zdarzeń w cyberprzestrzeni i przekształcono NCSC w centrum zdalnego zarządzania/reagowania na incydenty.

Finlandia

W wymiarze operacyjnym ochronę cyberprzestrzeni mają zapewnić poszczególne jednostki administracji w oparciu o przygotowane plany działania, które powstają na podstawie sporządzanych analiz ryzyka, które reguluje ustawa o ocenie bezpieczeństwa informacji (the Act on the Assessment of Information Security – 1406/2011)[2]. Analizę ryzyka zgodnie z ustawą może przeprowadzić narodowy regulator telekomunikacyjny (FICORA) bądź akredytowane przez regulatora jednostki. Centralny plan działania dla całej administracji został przyjęty w 2014 r. Pod auspicjami Ministerstwa Finansów funkcjonuje Zarząd Bezpieczeństwa Informacji Rządowej (The Government Information Security Management Board – VAHTI) koordynujący przekazywanie kluczowych informacji w zakresie centralnej administracji rządowej i wydawanie sektorowych wytycznych bezpieczeństwa.

[1] https://www.ncsc.nl/english/organisation

[2] http://www.finlex.fi/fi/laki/alkup/2011/20111406#Pidp3049664

Elementem działań operacyjnych jest budowa zdolności i rozwój monitoringu zagrożeń cyberprzestrzeni dotyczących kluczowych obszarów realizacji funkcji państwa w czasie rzeczywistym. W ramach struktury fińskiego regulatora rynku telekomunikacyjnego Viestintävirasto zostało powołane Centrum Cyberbezpieczeństwa (Cyber Security Centre). Centrum analizuje informacje od poszczególnych podmiotów z administracji i sektorów krytycznych dotyczące incydentów, głównych podatności, zakłóceń i ich efektów. Centrum współpracuje również z Policją, która jest właściwa do prowadzenia postępowań z zakresu cyberprzestępczości. Pod auspicjami Ministerstwa Finansów został również zainicjowany projekt budowy Security Operations Centre (SOC) w administracji centralnej - Central Government 24/7 Information Security Operations (SecICT). W skład SOC'a ma wejść m.in. rządowy CERT. Zakłada się wymianę informacji między Centrum a nowo tworzonym SecICT.

Kluczowym punktem strategii i przyjętych planów działania w zakresie cyberbezpieczeństwa jest także uruchomienie bezpiecznej sieci teleinformatycznej dla administracji publicznej (ustawa o TUVE), dzięki której można będzie przekazywać informacje dotyczące sektorów krytycznych, w tym informacje niejawne. Przesłanką utworzenia takiej sieci są korzyści centralizacji bezpieczeństwa teleinformatycznego. Fiński urząd ds. komunikacji elektronicznej, Viestintävirasto, zatrudnia około 240 osób.

Francja:

Francja jest jednym z pierwszych krajów, które podjęły działania legislacyjne w celu wzmocnienia swojego cyberbezpieczeństwa w dziedzinie infrastruktury usług kluczowych. Politykę państwa w zakresie ochrony systemów teleinformatycznych prowadzi premier za pośrednictwem Agencji Bezpieczeństwa Systemów Informacyjnych (Agence nationale de la sécurité des systèmes d'information "ANSSI"), zatrudniającej ok. 500 pracowników. Agencja dzięki pionowi operacyjnemu („operations room") i rozmieszczonym w ministerstwach sieciach typu „honey-pot" ma dostęp do bieżącej informacji na temat ataków i innych zagrożeń na poziomie centralnym; jednocześnie pełni rolę CSIRT odpowiedzialnego za obsługę incydentów i zagrożeń na szczeblu krajowym CERT-FR (CERT Narodowy).

Przepisy dotyczące bezpieczeństwa teleinformatycznego zostały wprowadzone do ustawy z dnia 18 grudnia 2013 r. o programowaniu wojskowym, która definiuje "operatorów o istotnym znaczeniu", zbliżonych do definicji "operatorów usług kluczowych" w dyrektywie 2016/1148/UE. Ustawa przewiduje, że operatorzy o istotnym znaczeniu powinni przestrzegać konkretnych środków bezpieczeństwa teleinformatycznego oraz są zobowiązani do zgłaszania incydentów do ANSSI. Agencja zapewnia wsparcie tym operatorom wydając wytyczne bezpieczeństwa teleinformatycznego. Agencja jest zaangażowana w koordynację implementacji dyrektywy 2016/1148/UE. Aktualne podejście do implementacji zakłada, że wymagania bezpieczeństwa dla operatorów usług kluczowych będą podobne jak dla operatorów infrastruktury krytycznej, a liczba operatorów usług kluczowych będzie wyższa niż liczba podmiotów objętych wymaganiami z zakresu infrastruktury krytycznej. We Francji obecnie zidentyfikowano ponad 200 operatorów infrastruktury krytycznej w 12 sektorach. ANSSI będzie wyznaczone zarówno jako pojedynczy punkt kontaktowy i organ właściwy w zakresie bezpieczeństwa sieci i informacji.

Niemcy:

Rozwiązania przewidziane w dyrektywie 2016/1148/UE zostały już wprowadzone w niemieckim porządku prawnym ustawą z dnia 25 lipca 2015 r. o zmianie ustawy z dnia 14 sierpnia 2009 r. o Federalnym Urzędzie ds. Bezpieczeństwa Informacji (*niem.* BSI). Ustawa zmienia istniejące ustawy o bezpieczeństwie infrastruktury krytycznej, prawie telekomunikacyjnym i inne, nie tworząc jednak spójnego systemu. Nałożyła na różne podmioty (przede wszystkim operatorów infrastruktury krytycznej i przedsiębiorców telekomunikacyjnych) nowe obowiązki dotyczące stosowania odpowiednich środków bezpieczeństwa, informowania klientów czy organów władzy publicznej o możliwych nadużyciach czy zagrożeniach. BSI dostał dodatkowe kompetencje w zakresie opracowywania standardów w zakresie cyberbezpieczeństwa, kontaktów z organami właściwymi.

BSI pełni funkcję federalnego urzędu ds. cyberbezpieczeństwa. Do jego zadań należy bieżąca analiza zagrożeń, przygotowywanie środków do ich zwalczania oraz zabezpieczanie przed nimi gospodarki. W ramach BSI funkcjonuje Cyber-Abwehrzentrum (Cyber-AZ), którego zadaniem jest koordynacja ochrony cyberprzestrzeni w Niemczech poprzez wczesne ostrzeganie, informację i prewencję. W stosowanie prawa dotyczącego bezpieczeństwa teleinformatycznego są zaangażowane ponadto Federalne Ministerstwo Spraw Wewnętrznych, Federalny Urząd Ochrony Ludności i Pomocy w przypadku Katastrof, kraje związkowe (landy), departamenty federalnych ministerstw: Transportu i Infrastruktury Cyfrowej, Gospodarki i Technologii, Edukacji i Nauki. Liczba operatorów usług kluczowych w Niemczech obejmuje ok. 1885 podmiotów, które są objęte dwoma pakietami rozporządzeń.

W Niemczech ustawa wprowadziła sektor spożywczy, niewystępujący w załączniku 2 dyrektywy 2016/1148/UE dyrektywy, natomiast nie objęła administracji publicznej, z uwagi na federalną strukturę państwa.

Niemiecki BSI zatrudnia w celu realizacji swoich zadań około 600 pracowników, a Cyber-AZ – 10 pracowników

delegowanych.

Stany Zjednoczone:

System bezpieczeństwa teleinformatycznego w Stanach Zjednoczonych jest opisany w wielu aktach prawnych. W Stanach Zjednoczonych odpowiednikiem europejskich regulacji z zakresu ochrony cyberprzestrzeni jest ustawa „Cyber Intelligence Sharing and Protection Act" z 2013 roku. Ustawa ma na celu zapewnienie wsparcia organom publicznym w zakresie zwiększenia odporności użytkowanych systemów teleinformatycznych oraz analizę zagrożeń pojawiających się w cyberprzestrzeni[3]. Ponadto istnieją ustawy o oszustwach i nadużyciach komputerowych, jak i dotyczące uzyskania nieautoryzowanego dostępu do komputera, zakłóceń, pozyskiwania danych oraz o ochronie prywatności w komunikacji elektronicznej[4]. Wydany został również Executive Order 13636/2013 – „Improving Critical Infrastructure Cybersecurity", który zidentyfikował 16 kluczowych obszarów infrastruktury oraz ustanowił organy nadzoru mające na celu poprawę bezpieczeństwa wśród podmiotów regulowanych. Założeniem amerykańskiego systemu cyberbezpieczeństwa jest silne partnerstwo publiczno-prywatne pomiędzy jednostkami administracji, środowiskiem naukowym i sektorem przedsiębiorstw w zakresie wymiany informacji na temat zagrożeń cyberprzestrzeni. Departament Bezpieczeństwa Wewnętrznego USA jest odpowiedzialny za sferę ochronę infrastruktury krytycznej – pod kątem zagrożeń fizycznych a także dotyczących cyberprzestrzeni. Ministerstwo udziela wsparcia dla operatorów infrastruktury krytycznej, publikuje również raporty nt. potencjalnych zagrożeń i podatności. Dodatkowo amerykański instytut zajmujący się standaryzacją NIST (National Institute of Standards and Technology) realizuje wiele uznanych międzynarodowo projektów zwiększenia cyberbezpieczeństwa infrastruktury krytycznej (bez konieczności dodatkowych zmian prawnych).

Ministerstwo posiada 24-godzinne Narodowe Centrum Koordynacji, Komunikacji i Cyberbezpieczeństwa - National Cybersecurity and Communications Integration Center (NCCIC) dysponujące kompleksową informacją na temat cyberbezpieczeństwa, reagujące na incydenty, zarządzające bezpieczeństwem teleinformatycznym. Centrum jest również punktem wymiany informacji z federalną administracją rządową, agencjami wywiadowczymi i organami ścigania. Działalność Centrum opiera się na dobrowolnej współpracy administracji publicznej i sektorów krytycznych. Centrum może również prowadzić działania proaktywne na rzecz zapobiegania incydentom w sieciach teleinformatycznych.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Przedsiębiorcy ogółem	1 840 000	Dane z raportu PARP, opracowane na podstawie danych GUS	Konieczność przeprowadzenia analizy, czy dostarczają usługi kluczowe
Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze elektroenergetycznym	20	Szacunki oparte na załączniku do projektu ustawy oraz danych URE (OSP, pięciu największych OSD dla gospodarstw domowych, dziewięciu największych OSD dla przedsiębiorców, pięciu największych sprzedawców prądu)	Spełnienie wymogów z art. 10, -16 projektu ustawy
Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze ropy naftowej	4	Szacunki oparte na załączniku do projektu ustawy oraz danych URE (OSP oraz czterej najwięksi przedsiębiorcy posiadający koncesję na dystrybucję, wytwarzanie, magazynowanie lub przeładunek paliw ciekłych oraz na obrót paliwami ciekłymi)	
Podmioty świadczące usługi kluczowe w sektorze	22	Szacunki oparte na załączniku do projektu ustawy oraz	

[3] https://en.wikipedia.org/wiki/Cyber-security_regulation

[4] https://www.rsaconference.com/writable/presentations/file_upload/law-w04-global_cybersecurity_laws_regulations_and_liability.pdf

energetycznym w podsektorze gazu		danych URE (OSP, OSD, przedsiębiorcy dostarczający lub magazynujący gaz lub gaz ziemny oraz dziesięć największych przedsiębiorstw gazowych w rozumieniu art. 2 pkt 1 dyrektywy 2009/73/WE)	
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu lotniczego	15	Szacunki oparte na załączniku do projektu ustawy oraz danych ULC (jeden przewoźnik lotniczy, zarządzający ośmioma największymi portami lotniczymi, pięć podmiotów obsługujących urządzenia pomocnicze znajdujące się w portach lotniczych oraz służba kontroli ruchu lotniczego)	
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu kolejowego	10	Szacunki oparte na załączniku do projektu ustawy oraz danych UTK (trzech największych zarządców infrastruktury kolejowej, czterech największych przewoźników kolejowych osobowych oraz trzech największych przewoźników kolejowych towarowych). Nie wzięto pod uwagę liczby operatorów infrastruktury usługowej ze względu na fakt, że rejestr obiektów infrastruktury usługowej zostanie utworzony przez Prezesa UTK do 30 czerwca 2018 r.	
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu wodnego (dotyczącym transportu morskiego)	17	Szacunki oparte na załączniku do projektu ustawy oraz danych MGMiŻŚ (założyliśmy objęcie dziesięciu największych armatorów, pięciu portów morskich oraz operatora SafeSeaNet)	
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu wodnego (dotyczącym transportu śródlądowego)	4	Szacunki oparte na załączniku do projektu ustawy oraz danych MGMiŻŚ (założyliśmy objęcie trzech największych armatorów i jednego portu śródlądowego)	
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu drogowego	24	Szacunki oparte na załączniku do projektu ustawy oraz danych MIiB (jeden zarządca dróg krajowych, szesnastu zarządców dróg wojewódzkich, dwóch operatorów systemów ITS na poziomie krajowym i pięciu w miastach).	

		Jest możliwe poszerzenie tej grupy o zarządców dróg powiatowych i gminnych, jednak nie były brane pod uwagę w szacunkach.	
Podmioty świadczące usługi kluczowe w sektorze bankowości i infrastruktury rynków finansowych	47	Szacunki oparte na załączniku do projektu ustawy oraz danych KNF (dwadzieścia największych banków, dziesięć największych banków spółdzielczych, Krajowa SKOK, dziesięć największych SKOK, dwa banki państwowe, jedna giełda, dwaj operatorzy systemu obrotu i jeden kontrahent centralny)	
Podmioty świadczące usługi kluczowe w sektorze zaopatrzenia w wodę pitną i jej dystrybucję	31	Przedsiębiorstwa wodno-kanalizacyjne na wykazie IK.	
Podmioty świadczące usługi kluczowe w sektorze służby zdrowia	131	Liczba podmiotów realizujących świadczenia szpitalne, które miały więcej niż 18 000 hospitalizacji rocznie (dane MZ) Dolnośląskie – 12 Kujawsko-Pomorskie – 8 Lubelskie – 8 Lubuskie – 3 Łódzkie – 8 Małopolskie – 10 Mazowieckie – 18 Opolskie – 3 Podkarpackie – 8 Podlaskie – 8 Pomorskie – 5 Śląskie – 15 Świętokrzyskie – 5 Warmińsko-mazurskie – 3 Wielkopolskie – 12 Zachodniopomorskie – 5	
Podmioty świadczące usługi kluczowe w sektorze infrastruktury cyfrowej	co najmniej 10	Szacunki oparte na analizie informacji rynkowych	
Dostawcy usług cyfrowych	co najmniej 25	Szacunki oparte na analizie informacji rynkowych	Spełnienie wymogów z art. 17-22 projektu ustawy
Naukowa i Akademicka Sieć Komputerowa	1	-	Przyjęcie roli CSIRT NASK wraz z zadaniami z zakresu cyberbezpieczeństwa określonymi w ustawie
Agencja Bezpieczeństwa Wewnętrznego	1	-	Przyjęcie roli CSIRT GOV wraz z zadaniami z zakresu cyberbezpieczeństwa określonymi w ustawie
Minister Obrony Narodowej	1	-	Przyjęcie roli CSIRT MON wraz z zadaniami z zakresu cyberbezpieczeństwa określonymi w ustawie
Podmioty świadczące usługi z zakresu	Co najmniej 30 podmiotów	Analiza własna na podstawie dostępnych publicznie ofert	Spełnienie wymogów z art. 15 ust. 2 projektu ustawy

cyberbezpieczeństwa		przedsiębiorców	
Centralna administracja rządowa	Ministerstwa (18) oraz jednostki im podległe i nadzorowane	-	Spełnienie wymogów z projektu ustawy
Terenowa administracja rządowa	Wojewodowie (16), ich jednostki podległe i nadzorowane, administracja zespolona i niezespolona w województwie	-	Spełnienie wymogów z projektu ustawy
Administracja samorządowa	Województwa (16), powiaty (314), miasta na prawach powiatu (66), gminy (2478)	Dane z GUS	Spełnienie wymogów z projektu ustawy
Organy właściwe w rozumieniu ustawy. W zakresie dla przedsiębiorców: Minister właściwy do spraw instytucji finansowych, minister właściwy do spraw informatyzacji, minister właściwy do spraw transportu, minister właściwy do spraw gospodarki morskiej i żeglugi śródlądowej, minister właściwy do spraw energii, minister właściwy do spraw zdrowia, minister właściwy do spraw środowiska	7	-	Wykonywanie zadań określonych w art. 38-40 projektu ustawy
Minister właściwy do spraw informatyzacji	1	-	Wykonywanie zadań z ustawy - art. 41 i art. 42 (możliwe upoważnienie jednostki nadzorowanej lub podległej); Prowadzenie pojedynczego punktu kontaktowego (art. 44); nadzór nad podmiotami świadczącymi usługi z zakresu cyberbezpieczeństwa (art. 47 ust. 1 pkt 1); prowadzenie wykazu usług kluczowych; prowadzenie wykazu operatorów usług kluczowych; prowadzenie rejestru poważnych incydentów. Realizacja funkcji organu właściwego dla sektora infrastruktury cyfrowej oraz dostawców usług cyfrowych – art. 38 ust. 1 pkt 7 i ust. 2 oraz art. 55 (funkcje mogą być powierzone podległym bądź nadzorowanym jednostkom organizacyjnym).
5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji			

Przeprowadzono ustalenia z ministerstwami, które uczestniczyły w pracach międzyresortowego zespołu roboczego ds. przygotowania ustawy (skład osobowy bazował na zespole ds. opracowania Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017-2022). Przeprowadzono również konsultacje wewnątrz resortu Ministerstwa Cyfryzacji.

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248), projekt ustawy zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Ministerstwa Cyfryzacji oraz na stronie Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny".

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	**0,00**	**1,76**	**1,80**	**1,80**	**1,80**	**1,80**	**1,80**	**1,80**	**1,80**	**1,80**	**1,80**	**17,96**
budżet państwa		1,02	1,02	1,02	1,02	1,02	1,02	1,02	1,02	1,02	1,02	10,20
JST	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
pozostałe jednostki (oddzielnie)	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Fundusz Ubezpieczeń Społecznych		0,38	0,41	0,41	0,41	0,41	0,41	0,41	0,41	0,41	0,41	4,07
Fundusz Pracy		0,14	0,14	0,14	0,14	0,14	0,14	0,14	0,14	0,14	0,14	1,40
Narodowy Fundusz Zdrowia		0,22	0,23	0,23	0,23	0,23	0,23	0,23	0,23	0,23	0,23	2,29
Wydatki ogółem	**1,92**	**19,95**	**16,8**	**16,01**	**26,04**	**26,04**	**26,04**	**26,04**	**26,04**	**26,04**	**26,04**	**236,96**
budżet państwa	1,92	19,95	16,8	16,01	26,04	26,04	26,04	26,04	26,04	26,04	26,04	236,96
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	**-1,92**	**-18,19**	**-15,00**	**-14,21**	**-24,24**	**-24,24**	**-24,24**	**-24,24**	**-24,24**	**-24,24**	**-24,24**	**-219,00**
budżet państwa	-1,92	-18,93	-15,78	-14,99	-25,02	-25,02	-25,02	-25,02	-25,02	-25,02	-25,02	-226,76
JST	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
pozostałe jednostki (oddzielnie)	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Fundusz Ubezpieczeń Społecznych	0,00	0,38	0,41	0,41	0,41	0,41	0,41	0,41	0,41	0,41	0,41	4,07
Fundusz Pracy	0,00	0,14	0,14	0,14	0,14	0,14	0,14	0,14	0,14	0,14	0,14	1,40
Narodowy Fundusz Zdrowia	0,00	0,22	0,23	0,23	0,23	0,23	0,23	0,23	0,23	0,23	0,23	2,29

Źródła finansowania	Budżet państwa – cz. 27 - Informatyzacja oraz rezerwa celowa (cz. 83 poz.19) pn. Rezerwa płacowa na zmiany organizacyjne i nowe zadania (w tym na skutki przechodzące z 2017 r.) oraz na wynagrodzenia osób zajmujących się programami finansowanymi z budżetu UE oraz środkami z pomocy udzielanej przez państwa członkowskie EFTA (w tym na niektóre skutki przechodzące z 2017 r.).
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Na potrzeby krajowego systemu cyberbezpieczeństwa przewiduje się wpływy do budżetu państwa z tytułu kar płaconych przez operatorów usług kluczowych (art. 57 ust. 2). Z tytułu art. 57 ust. 2 pkt 1-3 przyjęto liczbę kar na poziomie dwudziestu rocznie w każdej z kategorii, zaś z tytułu art. 57 ust. 2 pkt 4 i 5 oraz ust. 3 przyjęto liczbę kar na poziomie dwóch rocznie w każdej kategorii. Nie przewidziano wpływów do budżetu państwa od jednostek samorządu terytorialnego (JST), z uwagi na fakt, że JST realizują zadania wynikające z 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. W związku z tym, każda jednostka, która wdraża usługi świadczone drogą elektroniczną powinna dołożyć należytej staranności celem

zapewnienia ich bezpiecznego funkcjonowania. W procesie projektowym oraz utrzymania usług koszty te są naliczane normatywnie. Trzeba mieć także na uwadze, że JST, co do zasady mają zaimplementowany system zarządzania bezpieczeństwem informacji (SZBI) – dlatego też, zadania wynikające z art. 22 i 23 projektu ustawy będą realizowane w ramach SZBI.

Na potrzeby krajowego systemu cyberbezpieczeństwa powstanie system teleinformatyczny, który pozwoli na wymianę informacji o podatnościach, zagrożeniach i incydentach, jak również będzie zbierać informacje o poziomie ryzyka wystąpienia poważnego incydentu i prowadzić rejestr incydentów, w tym poważnych i krytycznych. System teleinformatyczny wesprze również agregację i korelację pozyskiwanych informacji w celu określenia: ryzyka wystąpienia incydentu, publikowania ostrzeżeń o zaistniałych incydentach, opracowania informacji o poziomie ryzyka dla RP jak również prognozę skutków materializacji zagrożeń cyberbezpieczeństwa. Koszt budowy systemu teleinformatycznego wyniesie ogólne 20.832.816,75 zł – finansowane z Narodowego Centrum Badań i Rozwoju. W rozbiciu na lata wyniesie to odpowiednio:

2017: 1 920 306,75 zł

2018: 10 185 015,00 zł

2019: 6 757 466,25 zł

2020: 1 970 028,75 zł

Ponadto, przewiduje się, że na utrzymanie systemu teleinformatycznego z budżetu państwa, części 27 - Informatyzacja, zostanie przeznaczone w 2020 r. (za okres IX-XII) 4 mln zł, a od 2021 po 16 mln zł rocznie.

Na koszty po stronie ministra właściwego do spraw informatyzacji składa się finansowanie zadań CSIRT NASK (corocznie 6,5 mln zł z budżetu państwa, części 27 - Informatyzacja) oraz nowych ustawowych zadań ministra właściwego do spraw informatyzacji (9 etatów opisanych poniżej). Realizacja przez Ministerstwo Cyfryzacji funkcji pojedynczego punktu kontaktowego (art. 38) wiąże się z koniecznością wzmocnienia kadrowego komórki odpowiedzialnej za te zadania. Niezbędne będzie stworzenie 5 stanowisk pracy dedykowanych do ww. zadań. Szacowany koszt jednostkowy uwzględniający zróżnicowanie stanowiskowe wynosi ok. 7 tys. brutto miesięcznie. Przewidziany koszt w 2018 r. to 372 tys. zł, a od 2019 r. 405 tys. zł rocznie.

W związku z realizacją przez Ministerstwo Cyfryzacji funkcji organu właściwego dla sektora infrastruktury cyfrowej i dostawców usług cyfrowych niezbędne będzie stworzenie po 4 stanowiska pracy dedykowane do ww. zadań. Szacowany koszt jednostkowy uwzględniający zróżnicowanie stanowiskowe wynosi ok. 7 tys. brutto miesięcznie. Przewidziany koszt w 2018 r. to 462 tys. zł, a od 2019 r. 501 tys. zł rocznie.

Uwzględniono także koszt stworzenia po cztery stanowiska pracy dedykowanych do ww. zadań w każdym z pozostałych organów właściwych (minister właściwy do spraw instytucji finansowych, minister właściwy do spraw transportu, minister właściwy do spraw gospodarki morskiej i żeglugi śródlądowej, minister właściwy do spraw energii, minister właściwy do spraw zdrowia, minister właściwy do spraw środowiska). Przewidziany koszt w 2018 r. to 2,235 mln zł, a od 2019 r. 2,425 mln zł rocznie.

Ze względu na nową formę raportowania do systemu teleinformatycznego przez prezesa UKE zakłada się utworzenie dwóch etatów. Szacowany koszt jednostkowy wynosie ok. 7 tys. brutto miesięcznie, co oznacza koszt w 2018 r. 196 tys. zł brutto, zaś od 2019 r. 212 tys. zł brutto. Wydatki na wynagrodzenia ww. pozostałych organów właściwych zostaną sfinansowane z rezerwy celowej (cz. 83 poz.19).

Dodatkowo, w części dotyczącej dochodów, uwzględniono wpływy z tytułu podatku dochodowego oraz składek, jak również wpływy z tytułu kar pieniężnych.

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								
	sektor przedsiębiorstw	0	1,06	2,11	2,06	2,06	2,11	19,85

pieniężnym (w mln zł, ceny stałe z 2017 r.)	– przedsiębiorcy, będący operatorami usług kluczowych – szacunkowy koszt dla przedsiębiorcy							
	sektor przedsiębiorstw – przedsiębiorcy, którzy chcą świadczyć usługi z zakresu cyberbezpieczeństwa – szacunkowy koszt dla przedsiębiorcy	0	2,06	2,06	2,06	2,06	2,06	20,6
W ujęciu niepieniężnym	duże przedsiębiorstwa	Operatorzy usług kluczowych będą zobowiązani do spełnienia wymogów określonych w ustawie (szczegółowy opis poniżej). Na marginesie warto zaznaczyć, że większość dużych przedsiębiorstw ma wdrożone już część rozwiązań ustawowych. Często te rozwiązania mają charakter sektorowy – jak CERT utworzony przez Polskie Sieci Elektroenergetyczne dla sektora energetycznego czy powstający CERT dla Związku Banków Polskich.						
	sektor mikro-, małych i średnich przedsiębiorstw	Operatorzy usług kluczowych będą zobowiązani do spełnienia wymogów określonych w ustawie. W zależności od tego czy będą to operatorzy usług kluczowych czy podmioty świadczące usługi z zakresu cyberbezpieczeństwa, obowiązki będą się różnić – szczegółowy opis poniżej.							
	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. Zwiększy się kontrola nad przebiegiem potencjalnych ataków (dzięki wprowadzeniu mechanizmów komunikowania się CSIRT krajowych między sobą). Część kosztów wypełnienia obowiązków ustawowych, w przypadku niektórych sektorów, może przełożyć się na wyższy koszt usługi dla odbiorcy końcowego.						

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 (operator usług kluczowych, dostawca usług cyfrowych, podmiot świadczący usługi z zakresu cyberbezpieczeństwa) i sektora. a) **Operatorzy usług kluczowych** – zwiększenie poziomu bezpieczeństwa świadczonych usług, poprzez wprowadzenie efektywnego zarządzania systemem cyberbezpieczeństwa, objęcie ochroną przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa. Nałożenie na operatorów dodatkowych obowiązków związanych z zapewnieniem bezpieczeństwa ich systemów informacyjnych, ciągłości świadczonych usług. Operatorzy usług kluczowych będą zobowiązani wskazać wśród swoich pracowników osobę odpowiedzialną za kwestie bezpieczeństwa teleinformatycznego. W przypadku konieczności zatrudnienia takiej osoby, przedsiębiorcy będą musieli się liczyć z kosztem od 5.000 zł do 10.000 zł brutto. Koszt jest zależny od kwalifikacji i obowiązków pracownika oraz od wielkości przedsiębiorcy. Koszt został policzony dla zatrudnienia 6 pracowników. Do tego należy doliczyć koszt utworzenia operacyjnego centrum bezpieczeństwa (SOC) – szacunkowo 1 mln zł oraz jego utrzymania – szacunkowo 2 mln zł, przy czym kwota ta może się zmienić w przypadku utworzenia sektorowego SOC albo skorzystania z komercyjnych usług podmiotu działającego na rynku. Operatorzy usług kluczowych będą zobowiązani m.in. ponieść koszty audytu zewnętrznego raz na dwa lata. Szacuje się, że koszt jednostkowy wykonania audytu wyniesie 50 tys. zł. Audyt po raz pierwszy będzie przeprowadzony w roku 2019 a następnie co 2 lata. a. Sektor energetyka, podsektor energia elektryczna Podsektor tworzą duże przedsiębiorstwa obsługujące wiele podmiotów, korzystające z systemów informacyjnych w znacznym stopniu. Wdrożenie regulacji przyczyni się do zapewnienia ciągłości dostaw prądu, zwiększy odporność przedsiębiorstw na ataki na

	infrastrukturę teleinformatyczną. Regulacja obejmie operatorów sieci przesyłowej (jest to jedna firma – Polskie Sieci Energetyczne S.A.), operatorów sieci dystrybucji: pięciu znaczących dla rynku gospodarstw domowych (Innogy Stoen Operator Sp. z o.o, PGE Dystrybucja S.A., ENEA Operator Sp. z o.o., Tauron Dystrybucja S.A., ENERGA – Operator S.A.), dziewięciu największych dla rynku przedsiębiorstw (m.in. dla portów morskich oraz największych przedsiębiorstw); oraz sprzedawców – według danych URE najwięksi sprzedawcy to podmioty należące do tych samych grup kapitałowych, co najwięksi dystrybutorzy. b. Sektor energetyka, podsektor ropa naftowa Podsektor tworzą duże przedsiębiorstwa, korzystające z systemów informacyjnych. Wdrożenie regulacji ustawowych przyczyni się do poprawy bezpieczeństwa i stworzenia systemu odpornego na ataki. Regulacja obejmie: operatora ropociągów (PERN S.A.); przedsiębiorstwa zajmujące się wydobyciem, przetwarzaniem, magazynowaniem i przesyłem ropy naftowej (Polskie Górnictwo Naftowe i Gazownictwo i LOTOS Petrobaltic S.A.) oraz rafinerie (PKN „Orlen", Grupa LOTOS S.A.). c. Sektor energetyka, podsektor gazu Podsektor tworzą duże przedsiębiorstwa, korzystające z systemów informacyjnych. Wdrożenie regulacji będzie miało znaczenie dla zapewnienia ciągłości dostaw do odbiorców końcowych. Regulacja obejmie przedsiębiorstwa dostarczające gaz, operatorów systemu dystrybucji (m.in. PSG sp. z o.o.), operatora systemu przesyłowego (w Polsce tą funkcję pełni Gaz-System S.A), operatorów systemu magazynowania (PGNiG, który obsługuje siedem największych magazynów gazu w Polsce), operator systemu LNG (także jest Gaz-System S.A.), a także operatora instalacji służących do rafinacji i przetwarzania gazu ziemnego (również PGNiG). d. Sektor transport, podsektor transport lotniczy Główne podmioty tworzące sektor skorzystają na włączeniu ich w system cyberbezpieczeństwa – zyskają ochronę przed skutkami ataków na infrastrukturę cyfrową, a także informacje na temat zagrożeń. Regulacja obejmie: jednego przewoźnika lotniczego, zarządców portów lotniczych (w Polsce działa 8 bazowych dla sieci europejskiej portów w rozumieniu rozporządzenia UE 1315/2013) a także instytucję zapewniającą służbę żeglugi powietrznej, o której mowa w art. 127 ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze. e. Sektor transport, podsektor transport kolejowy Podsektor jest zróżnicowany, jednak mające kluczowe znaczenie przedsiębiorstwa działają na rynku od lat i korzystają w znacznym stopniu z systemów informacyjnych. Włączenie ich w system cyberbezpieczeństwa przyczyni się do zwiększenia bezpieczeństwa świadczonych usług. Regulacja obejmie: zarządców infrastruktury kolejowej – głównie PKP Polskie Linie Kolejowe S.A., przedsiębiorstwa kolejowe, obsługujące zarówno transport pasażerski (Przewozy Regionalne, Koleje Mazowiecki, PKP SKM Śródmieście, PKP Intercity), jak i transport towarowy (m.in. PKP Cargo, DB Cargo Polska). Regulacja obejmie także operatorów obiektów infrastruktury usługowej, gdy tylko zostaną zidentyfikowani w rejestrze Prezesa Urzędu Transportu Kolejowego. f. Sektor transport, podsektor transport wodny Główne podmioty zyskają na włączeniu ich do systemu cyberbezpieczeństwa a bezpieczeństwo świadczonych przez nie usług będzie wyższe. Regulacja obejmie armatorów, organy zarządzające portami (regulacja ma na celu objąć zwłaszcza organy zarządzające portami morskimi w Gdyni, Gdańsku, Szczecinie, Elblągu, Kołobrzegu) oraz portami śródlądowymi, a także operatorów systemów ruchu

	statków. g. Sektor transport, podsektor transport drogowy Zadania wykonywane przez rodzaje podmiotów określone w dyrektywie są zarządzane przez administrację publiczną. Zadania w przypadku inteligentnych systemów transportowych (ITS) są często zlecane przedsiębiorstwom. Rozwiązania ustawowe wprowadzą regulacje dotyczące bezpieczeństwa systemów informacyjnych, które do tej pory były realizowane w zależności od podmiotu i cechował je brak jednolitości. Regulacja obejmie organy administracji drogowej – Generalną Dyrekcję Dróg Krajowych i Autostrad oraz samorządy, operatorów inteligentnych systemów transportowych. h. Sektor bankowość i infrastruktura rynków finansowych, podsektor bankowość W dużej mierze podmioty świadczące usługi bankowe są świadome znaczenia cyberbezpieczeństwa. Podwaliny pod to położyła rekomendacja D Komisji Nadzoru Finansowego dotycząca zarządzania ryzykiem towarzyszącym systemom informatycznym i telekomunikacyjnym używanym przez banki. Niniejsza regulacja obejmie przede wszystkim duże banki, a decydujące znaczenie będzie miało określenie progów kwalifikacyjnych w rozporządzeniu. i. Sektor bankowość i infrastruktura rynków finansowych, podsektor infrastruktura rynków finansowych Podmioty tworzące sektor to duże przedsiębiorstwa o stabilnej sytuacji rynkowej, które podobnie jak sektor bankowy objętą są stosownymi rekomendacjami Komisji Nadzoru Finansowego. Regulacja obejmie operatora systemu obrotu, czyli Giełdę Papierów Wartościowych i jej spółki zależne, oraz kontrahentów centralnych. j. Sektor służba zdrowia Sektor służby zdrowia w Polsce ma charakter rozproszony, a zapewnienie ciągłości działania w tym sektorze ma szczególne znaczenie dla funkcjonowania całego państwa. Sprostanie regulacjom pozwoli na zapewnienie ciągłości działania usługi zależnych od systemów informacyjnych, która ma kluczowe znaczenie dla życia i zdrowia obywateli. Regulacja obejmie rozproszone podmioty różnego rodzaju, zarówno z sektora publicznego, jak i prywatnego. Część podmiotów może być prowadzona przez organizacje pożytku publicznego. k. Sektor zaopatrzenia w wodę i jej dystrybucja Sektor jest rozproszony, trudno ocenić obecny stan zabezpieczenia. Z uwagi na charakter sektora – dodatkowe koszty mogą stanowić problem, zwłaszcza gdyby miały być przerzucone na odbiorców (niechęć do zwiększenia kosztów dostaw wody i odbioru ścieków). Wdrożenie systemu cyberbezpieczeństwa pozwoli zabezpieczyć kluczową usługę z punktu widzenia życia i zdrowia obywateli. Regulacja obejmie przedsiębiorstwa wodno-kanalizacyjne. Dostarczanie wody pitnej i odbiór ścieków to zadania własne gmin i powiatów. l. Sektor infrastruktura cyfrowa Podmioty tworzące sektor są świadome znaczenia cyberbezpieczeństwa. Wdrożenie regulacji ustawowych zapewni lepszą komunikację między nimi i ustandaryzowanie bezpieczeństwa sieci teleinformatycznych. Regulacja obejmie NASK (jako podmiot obsługujący Domain Name System i Top Level Domain), a także podmioty obsługujące IXP – cztery największe podmioty. b) **Dostawcy usług cyfrowych** – ze względu na brak wydanej decyzji wykonawczej Komisji Europejskiej, nie jest obecnie możliwe jednoznaczne określenie wpływu regulacji na sytuację dostawców usług cyfrowych. Sama ustawa nakłada na dostawców usług cyfrowych głównie wymogi sprawozdawcze wobec CSIRT prowadzonego przez ministra właściwego do spraw cyfryzacji oraz uprawnienia nadzorcze ex post organu właściwego. c) **Podmioty świadczące usługi z zakresu cyberbezpieczeństwa** – ustawa zwiększy zapotrzebowanie na usługi tego typu podmiotów. Nałoży na nie także obowiązki, które

	przyczynią się do wzrostu wiarygodności podmiotów i pozwolą na lepszą komunikację miedzy nimi (która z kolei przyczyni się do ograniczenia rozprzestrzeniania się incydentów). Przedsiębiorcy, którzy będą chcieli świadczyć usługi z zakresu cyberbezpieczeństwa (dla operatorów usług kluczowych) będą ponosili koszty: z tytułu utworzenia/dostosowania podmiotu do wymogów ustawy/rozporządzenia 1 mln zł, utrzymania zdolności (2 mln zł rocznie) oraz zatrudnienia wykwalifikowanej kadry (koszt 0,6 mln rocznie dla jednostki). Powyższe koszty mogą się różnić w zależności od wybranego wariantu działania. Podmiot może świadczyć wybrane usługi z katalogu usług cyberbezpieczeństwa. Np. same usługi z zakresu reagowania na incydenty, usługi z zakresu reagowania na incydenty i SOC, usługi audytowe itp.).

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:

Realizacja zamierzeń ustawy wymaga wykonywania przez przedsiębiorstwa obowiązków, takich jak ochrona swoich systemów informacyjnych, zapewnianie cyberbezpieczeństwa i monitorowanie świadczonych usług kluczowych, zorganizowanie ścisłej współpracy z CSIRT i odpowiednimi urzędami, w tym wymiana informacji dotyczącej incydentów; analiza, dokumentacja, rejestracja, naprawianie, usuwanie przyczyn, objęcie ochroną usługi kluczowe i prognozowanie skutków materializacji zagrożeń cyberbezpieczeństwa oraz informowanie użytkownika usług kluczowych o możliwych zagrożeniach.

9. Wpływ na rynek pracy

Z najnowszego raportu firmy analitycznej IDC wynika, że wartość sektora zajmującego się cyberbezpieczeństwem w ciągu roku wzrosła o ponad 7 proc., w związku z tym polski rynek rozwiązań bezpieczeństwa IT rozwija się niezwykle dynamicznie i nowi eksperci będą pojawiać się na rynku. Rosnący popyt będzie napędzany w znacznej mierze przez inwestycje ze strony sektora publicznego i prywatnego. Wzrośnie zapotrzebowanie w szczególności na specjalistów w dziedzinie bezpieczeństwa IT/ICT oraz specjalistów bezpieczeństwa przy systemach Operational Technology (np. SCADA).

Ustawa usankcjonuje utworzenie u operatora usługi kluczowej stanowiska ds. cyberbezpieczeństwa oraz wpłynie na certyfikację tego typu kompetencji. Ponadto ustawa umożliwi rozwój przedsiębiorstw zajmujących się ochroną systemów informacyjnych.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☒ informatyzacja ☒ zdrowie

Omówienie wpływu	Projekt spełnia wymagania interoperacyjności, czyli zdolność systemów teleinformatycznych do efektywnej współpracy w celu zapewnienia wzajemnego dostępu użytkowników do usług świadczonych w tych sieciach.

	Projekt spełnia również wymogi neutralności technologicznej, wykorzystania danych z rejestrów publicznych oraz ochrony danych osobowych, co znalazło wyraz w konstrukcji przepisów szczegółowych, odnoszących się zwłaszcza do funkcjonalności systemów informacyjnych budowanych na potrzeby ustawy oraz sposobu przetwarzania danych w tych systemach. Zakresem ustawy będą również objęte najważniejsze podmioty w służbie zdrowia, co przyczyni się do poprawy ciągłości działania użytkowanych systemów teleinformatycznych służących świadczeniu usług kluczowych w tym sektorze.

11. Planowane wykonanie przepisów aktu prawnego

Celem zapewnienia niezakłóconego świadczenia usług kluczowych i usług cyfrowych oraz osiągnięcia odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do ich świadczenia założeniem projektodawcy jest po pierwsze stworzenie przepisów i procedur służących zapewnieniu cyberbezpieczeństwa w podmiotach zobowiązanych, czyli u operatorów usług kluczowych oraz struktur i rozwiązań systemowych odpowiedzialnych za zarządzanie cyberbezpieczeństwem w skali kraju. Ostatnim elementem projektu ustawy jest uruchomienie systemu teleinformatycznego umożliwiającego zbieranie informacji od podmiotów zobowiązanych i zarządzanie krajowym systemem cyberbezpieczeństwa.

W pierwszej kolejności zostaną przyjęte przez organy właściwe rekomendacje sektorowe w zakresie wzmocnienia cyberbezpieczeństwa. Rekomendacje powinny zawierać wytyczne sektorowe dotyczące rejestracji/zgłaszania, incydentów do krajowym systemie cyberbezpieczeństwa. Powyższe umożliwi określenie w wymiarze sektorowym elementów systemu zarządzania bezpieczeństwem, do których zobowiązani są operatorzy usług kluczowych na podstawie art. 10 projektu ustawy. W pracach mogą zostać wykorzystane dotychczasowe dobre praktyki w tym, zakresie, a więc Rekomendacja D[5] dotycząca zarządzania ryzykiem towarzyszącym systemom informatycznym i telekomunikacyjnym używanym przez banki, przepisy rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ramach Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*[6], wymagania bezpieczeństwa teleinformatycznego odnoszące się do sfery infrastruktury krytycznej[7]. Forma prawna jakimi są rekomendacje zapewnia neutralność technologiczną wobec zmian środowiska normalizacyjnego z zakresu zarządzania bezpieczeństwem informacji, z drugiej strony będzie zbieżna z innymi regulacjami ze sfery cyberbezpieczeństwa, a więc np. ustawy z dnia 5 września 2016 r. *o usługach zaufania i identyfikacji elektronicznej* – art. 39[8]. Uzupełnieniem wymagań sektorowych będą przepisy decyzji wykonawczej Komisji Europejskiej odnoszące się do dostawców cyfrowych. Częścią prac sektorowych, jest zainicjowanie przez ministra właściwego do spraw informatyzacji prac nad ustaleniem progów istotności skutku zakłócającego dla świadczenia usług kluczowych pozwalających na uznanie usługi za usługę kluczową. Prace nad progami, winny być zakończone przed 1 lipca 2018 r.. tak aby możliwe było zidentyfikowanie przez organy właściwe operatorów usług kluczowych. W ramach prac sektorowych opracowywane będą również przepisy rozporządzenia Rady Ministrów odnoszące się do zakresu informacji, które powinny zawierać dokumentacja cyberbezpieczeństwa.

Równocześnie z pracami dotyczącymi sektorów będą prowadzone prace nad nowymi rozwiązaniami systemowymi i strukturami zajmującymi się cyberbezpieczeństwem na poziomie technicznym oraz zainicjowaniem działań przez pojedynczy punkt kontaktowy. Zgodnie z przepisami ustawowymi rolę pojedynczego punktu kontaktowego ds. cyberbezpieczeństwa będzie pełnić minister właściwy ds. informatyzacji.

Ostatnim elementem projektu ustawy jest uruchomienie ustawowych zadań zespołów realizujących zadania CSIRT poziomu krajowego oraz systemu teleinformatycznego wspierającego realizację zadań przez podmioty wchodzące w skład krajowego systemu cyberbezpieczeństwa. Przepisy ustawy przewidują 3-miesięczne vacatio legis dla zapewnienia pełnej funkcjonalności przez zespoły tworzące CSIRT poziomu krajowego. Z drugiej strony przewidziane jest uruchomienie systemu teleinformatycznego który zapewni realizację funkcji narodowego centrum cyberbezpieczeństwa. Projekt ustawy zakłada uruchomienie z dniem 1 września 2020 r. systemu teleinformatycznego wspierającego realizację zadań podmiotów krajowego systemu cyberbezpieczeństwa, w szczególności umożliwiającego:

1) Zgłaszanie i obsługę incydentów,
2) Szacowanie ryzyka teleinformatycznego

[5] Wydana przez Komisję Nadzoru Finansowego w styczniu 2013r., na podstawie art. 137 pkt 5 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2012 r. poz. 1376 j.t. z późn. zm.).

[6] Dz. U. z 2012 r. Nr 526 z późn. zm.

[7] Zawarte w załączniku nr 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK), przyjmowanego na podstawie ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 j.t.).

[8] Dz. U. z 2016 r. poz. 1579.

3) Ostrzeganie o zagrożeniach cyberbezpieczeństwa.

Ponadto, aby zapewnić spójność krajowego systemu cyberbezpieczeństwa przewidzianego w projekcie ustawy koniecznym jest włączenie przedsiębiorców telekomunikacyjnych, którzy realizują obowiązki z zakresu cyberbezpieczeństwa określone w ustawie – Prawo telekomunikacyjne.

Celem zminimalizowani obciążeń dla operatorów usług kluczowych, projekt ustawy przewiduje, że w przypadku gdy operator usługi kluczowej jest równocześnie właścicielem, posiadaczem samoistnym i zależnym obiektów, instalacji lub urządzeń infrastruktury krytycznej i posiada plan ochrony infrastruktury krytycznej, o którym mowa w art. 6 ust. 5 ustawy o zarządzaniu kryzysowym, nie jest on zobowiązany do przygotowania dodatkowej dokumentacji dotyczącej cyberbezpieczeństwa systemów wykorzystywanych do świadczenia usług kluczowych, zgodnie z zakresem informacji określonym w przepisach wydanych na podstawie art. 10 ust. 3 projektowanej ustawy. Jednakże uwzględnia on informacje z zakresu cyberbezpieczeństwa w swoim planie ochrony infrastruktury krytycznej.

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

1. Zgodność z ustawą. Częstotliwość pomiaru: 1 / 2 lata od wejścia ustawy w życie. Źródło pomiaru: wyniki audytów.
2. Jakość zabezpieczeń. Częstotliwość pomiaru: 1 / rok od wejścia ustawy w życie. Źródło pomiaru: raporty CSIRT, ćwiczenia.
3. Skuteczność zarządzania incydentami. Częstotliwość pomiaru: 1 / rok od wejścia ustawy w życie. Źródło pomiaru: czas od momentu zaistnienia zdarzenia do czasu jego wykrycia w systemie.
4. Przegląd poważnych incydentów. Częstotliwość pomiaru: 2 / rok od wejścia ustawy w życie. Źródło pomiarów: rejestr poważnych incydentów (w tym ilość zgłaszających, ilość poważnych incydentów, ilość operatorów usług kluczowych).
5. Dostępność usług świadczonych przez operatorów usług kluczowych. Częstotliwość pomiaru: 1 / rok od wejścia ustawy w życie. Źródło pomiaru: dziennik awarii systemów informacyjnych służących do świadczenia usług kluczowych.
6. Zwiększenie świadomości: Częstotliwość pomiaru: 1 / rok od wejścia ustawy w życie. Źródło pomiaru: plany szkoleń i przeprowadzone kampanie społeczne.

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