Projekt z dnia 30 maja 2018 r.

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia ……..... 2018 r.

w sprawie progów uznania incydentu za poważny[1)]

Na podstawie art. 11 ust. 4 ustawy z dnia……. 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …..) zarządza się, co następuje:

§ 1. Określa się progi uznania incydentu za poważny według rodzaju zdarzenia w poszczególnych sektorach i podsektorach określonych w załączniku nr 1 do ustawy z dnia …….. 2018 r. o krajowym systemie cyberbezpieczeństwa, stanowiące załącznik do rozporządzenia.

§ 2. Rozporządzenie wchodzi w życie z dniem……... 2018 r.

PREZES RADY MINISTRÓW

ZA ZGODNOŚĆ POD WZGLĘDEM PRAWNYM,
REDAKCYJNYM I LEGISLACYJNYM
Katarzyna Prusak-Górniak
Dyrektor Departamentu Prawnego
w Ministerstwie Cyfryzacji
/- podpisano elektronicznie/

[1)] Niniejsze rozporządzenie w zakresie swojej regulacji wdraża dyrektywę 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).

Załącznik do rozporządzenia
Rady Ministrów
z dnia ……2018 r. (poz. …)

Sektor	Podsektor	Zdarzenie	Progi
Energia	Wydobywanie kopalin	Incydent dotyczący wydobywania kopalin.	1. Incydent doprowadził do przerwania wydobycia na dłużej niż 12 godzin. 2. Incydent spowodował ryzyko utraty zdrowia lub życia ludzi. 3. Incydent spowodował straty finansowe przekraczające 100 000 złotych.
	Energia elektryczna	Incydent dotyczący obciążenia obszarów synchronizowanych.	1. Energia nie dostarczona po rozłączeniu synchronizacji odpowiada od 1 do 10% szacowanego obciążenia operatora systemu przesyłowego bezpośrednio przed wystąpieniem incydentu. 2. Incydent trwa dłużej niż trzy minuty. 3. Rozłączenie synchronizacji jest większe niż 200 MW.
		Incydent dotyczący obciążenia.	Zmniejszenie obciążenia od 5 do 15% w czasie trwania incydentu, niezależnie od czasu trwania incydentu.
		Incydent dotyczący elementów sieci przesyłowej.	Końcowe wyłączenie samoczynne lub ręczne awaryjne rozłączenie sprzętu zasilającego znajdującego się na liście rezerwowej przeznaczonych na wypadek sytuacji wyjątkowych i wywołujące skutki w obszarze odpowiedzialności i/lub dla przesyłu transgranicznego.
		Incydent dotyczący zmniejszenia możliwości operacyjnych.	Operator systemu przesyłowego traci kontrolę nad systemami sterowania na dłużej niż 30 minut.
		Incydent dotyczący niezawodności oddzielenia od zasilania.	Incydent prowadzi do wydzielenia istotnych części od zasilania, w którego skład wchodzi co najmniej jeden obszar odpowiedzialności operatora systemu przesyłowego.
		Incydent dotyczący utraty kontroli nad systemami sterowania.	Operator systemu przesyłowego całkowicie utracił kontrolę nad systemami sterowania na dłużej niż 30 minut.
		Incydent blackoutu (przerwania dostawy energii elektrycznej) dla obszarów	Operator systemu przesyłowego: 1) ogłosił blackout (przerwanie dostawy energii elektrycznej); 2) utracił synchronizację na ponad

		synchronizowanych.	50% obszaru odpowiedzialności; 3) miał całkowitą utratę napięcia w systemie na dłużej niż 3 minuty.
		Incydent blackoutu (przerwania dostawy energii elektrycznej) dla systemów wyizolowanych.	Utrata 70% synchronizacji w czasie incydentu lub całkowita utrata mocy.
	Ciepło	Incydent dotyczący wytwarzanie ciepła.	Incydent skutkuje niemożnością prawidłowej realizacji procesu wytwarzania ciepła.
		Incydent dotyczący obrotu ciepłem.	Incydent skutkuje niemożnością prawidłowej realizacji procesu przesyłania ciepła.
		Incydent dotyczący przesyłania ciepła.	Incydent skutkuje niemożnością prawidłowej realizacji procesu dystrybucji ciepła.
		Incydent dotyczący dystrybucji ciepła.	Incydent skutkuje niemożnością prawidłowej realizacji procesu obrotu ciepła.
	Ropa naftowa i Gaz	Incydent dotyczący przesyłu ropy naftowej, paliw ciekłych i gazu ziemnego rurociągami.	1. Nieplanowany wyciek ropy naftowej, gazu lub innych substancji niebezpiecznych, niezależnie od tego, czy doszło do zapłonu. 2. Incydent skutkuje niemożliwością prawidłowego dostarczania i przesyłu ropy naftowej i gazu ziemnego.
		Incydent dotyczący produkcji, wydobywania, wytwarzania paliw ciekłych, magazynowania ropy naftowej, przeładunku ropy naftowej, magazynowania paliw ciekłych, przeładunku paliw ciekłych, obrotu paliwami ciekłymi i obrotu paliwami ciekłymi z zagranicą, wytwarzania paliw syntetycznych.	1. Znacząca utrata integralności, lub utrata ochrony przeciwko efektom eksplozji, lub utrata stacji utrzymania w przypadku instalacji mobilnych. 2. Incydent skutkuje zakłóceniem w produkcji, rafinacji, funkcjonowaniu urządzeń przetwarzających, magazynowaniu i przesyłaniu ropy naftowej.
		Incydent dotyczący przedsiębiorstw zajmujących się wytwarzaniem paliw gazowych, przesyłaniem paliw gazowych,	1. Nieplanowany wyciek gazu lub innych substancji niebezpiecznych, niezależnie od tego, czy doszło do zapłonu, znacząca utrata integralności, lub utrata ochrony przeciwko efektom eksplozji, lub utrata

		dystrybucją paliw gazowych, obrotem paliwami gazowymi i obrotem gazem ziemnym z zagranicą, magazynowaniem paliw gazowych, skraplaniem i regazyfikacją LNG oraz sprowadzaniem i wyładunkiem LNG.	stacji utrzymania w przypadku instalacji mobilnych. 2. Incydent skutkuje niemożliwością prawidłowego dostarczania i przesyłu gazu ziemnego, a także zakłóceniem w produkcji, funkcjonowaniu urządzeń przetwarzających, magazynowaniu i przesyłaniu gazu ziemnego.
	Dostawy i usługi dla sektora energii	Incydent dotyczący dostaw systemów, maszyn, urządzeń, materiałów, surowców oraz świadczenia usług na rzecz sektora energii.	Incydent skutkuje niemożnością prawidłowej realizacji procesu dostawy i świadczenia usługi na rzecz sektora energii.
		Incydent dotyczący utrzymywania rezerw strategicznych i zapasów ropy naftowej, produktów naftowych i gazu ziemnego.	Incydent skutkuje niemożnością prawidłowej realizacji procesu udostępniania rezerw strategicznych lub uwalniania zapasów ropy naftowej, produktów naftowych i gazu ziemnego.
		Incydent dotyczący unieszkodliwiania odpadów promieniotwórczych.	Incydent skutkuje niemożnością prawidłowej realizacji procesu unieszkodliwiania odpadów promieniotwórczych.
Transport	Transport lotniczy	Incydent dotyczący transportu lotniczego pasażerskiego.	1. Przerwanie realizacji usług przez przewoźnika na czas dłuży niż 4 godziny. lub 2. Uszkodzenie statku powietrznego lub systemów informacyjnych kluczowych dla jego sterowania i funkcjonowania. lub 3. Incydent doprowadził do uruchomienia procedur zarządzania kryzysowego. lub 4. Incydent spowodował narażenie na utratę życia lub zdrowia obsługiwanych pasażerów lub personelu.
		Incydent dotyczący transport lotniczego towarów.	1. Przerwanie realizacji usług przez przewoźnika na czas dłuży niż 4 godziny. lub 2. Uszkodzenie statku powietrznego lub systemów informacyjnych kluczowych dla jego sterowania i

			funkcjonowania. lub 3. Incydent doprowadził do uruchomienia procedur zarządzania kryzysowego. lub 4. Incydent spowodował narażenie na utratę życia lub zdrowia obsługiwanych pasażerów lub personelu.
		Incydent dotyczący działalności usługowej wspomagającej transport lotniczy.	1. Przerwanie realizacji procesu kontroli bezpieczeństwa przez zarejestrowanego agenta na czas dłuższy niż 4 godziny. lub 2. Zakłócenie wykonywania usług przekazu informacji o statusie ochrony nadanym przesyłce na czas dłuższy niż 4 godziny.
			Incydent doprowadził do braku dostępności usługi wykonywanych przez agenta handlingowego na czas dłuższy niż 4 godziny lub negatywnie wpłynął na usługi wykonywane przez inne podmioty w podsektorze.
			1. Zakłócenie wykonywania operacji lotniczych na czas dłuższy niż 4 godziny. lub 2. Incydent spowodował narażenie na utratę życia lub zdrowia obsługiwanych pasażerów lub personelu. lub 3. Incydent doprowadził do uruchomienia procedur zarządzania kryzysowego. lub 4. Wiedza o incydencie jest powszechnie dostępna lub incydent mógł spowodować istotną szkodę wizerunkową. lub 5. Incydent doprowadził do braku dostępności usługi i negatywnie wpłynął na usługi wykonywane przez inne podmioty w podsektorze.
		Incydent dotyczący instytucji zapewniającej służby żeglugi powietrznej.	Incydent doprowadził do zakłócenia systemu zarządzania ruchem lotniczym i ograniczenia przepustowości przestrzeni

			powietrznej o co najmniej 30%.
	Transport kolejowy	Incydent dotyczący konstrukcji rozkładu jazdy pociągów.	1. Brak możliwości konstrukcji rozkładów jazdy pociągów wynikająca z: a) działania złośliwego oprogramowania (cyberatak), b) braku zasilania energetycznego powodujący niedostępność usługi powyżej 12 godzin, c) awarii sieci teleinformatycznych powyżej 12 godzin. 2. Brak możliwości uruchomienia pociągów i prowadzenia ruchu kolejowego spowodowany brakiem możliwości konstrukcji rozkładu jazdy powyżej 12 godzin.
		Incydent w transporcie kolejowym pasażerskim.	1. Przerwanie realizacji usług przez przewoźnika na czas dłuży niż 2 godziny. lub 2. Uszkodzenie pojazdu szynowego lub systemów informacyjnych kluczowych dla jego sterowania i funkcjonowania lub 3. Incydent doprowadził do uruchomienia procedur zarządzania kryzysowego. lub 4. Wypadek z przynajmniej jednią ofiarą śmiertelną lub przynajmniej 5 ciężko rannymi osobami.
		Incydent w transporcie kolejowym towarów.	1.Przerwanie realizacji usług przez przewoźnika na czas dłuży niż 6 godzin. lub 2.Uszkodzenie pojazdu szynowego lub systemów informacyjnych kluczowych dla jego sterowania i funkcjonowania. lub 3.Incydent doprowadził do uruchomienia procedur zarządzania kryzysowego. lub 4. Wypadek z przynajmniej jedną ofiarą śmiertelną lub przynajmniej 5 ciężko rannymi osobami. lub 5. Wypadek z udziałem co najmniej

			jednego pojazdu szynowego transportującego niebezpieczne towary, w którym doszło do uwolnienia substancji niebezpiecznych.
	Transport wodny	Incydent dotyczący armatorów w transporcie morskim pasażerów.	1. Uszkodzenie lub awaria systemów informacyjnych kluczowych dla sterowania i funkcjonowania statku. 2. Uszkodzenie kadłuba statku. 3. Zalanie bądź zatopienie statku. 4. Kolizja statku. 5. Wywrócenie lub przechył statku. 6. Utrata kontroli nad statkiem.
		Incydent dotyczący armatorów w transporcie morskim towarów.	1. Uszkodzenie lub awaria systemów informacyjnych kluczowych dla sterowania i funkcjonowania statku. 2. Uszkodzenie kadłuba statku. 3. Zalanie bądź zatopienie statku. 4. Kolizja statku. 5. Wywrócenie lub przechył statku. 6. Utrata kontroli nad statkiem.
		Incydent dotyczący armatorów w transporcie wodnym śródlądowym pasażerskim.	1. Zniszczenie statku lub systemów informacyjnych kluczowych dla sterowania i funkcjonowania statku. 2. Zdarzenie związane z ruchem lub postojem statku, którego następstwem jest śmierć człowieka. 3. Pożar lub wybuch na statku. 4. Wypadek żeglugowy z udziałem co najmniej jednego statku.
		Incydent dotyczący armatorów w transporcie wodnym śródlądowym towarów.	1. Zniszczenie statku lub systemów informacyjnych kluczowych dla sterowania i funkcjonowania statku. 2. Zdarzenie związane z ruchem lub postojem statku, którego następstwem jest śmierć człowieka. 3. Pożar lub wybuch na statku. 4. Wypadek żeglugowy z udziałem co najmniej jednego statku. 5. Wypadek żeglugowy z udziałem co najmniej jednego statku transportującego niebezpieczne towary, w których doszło do uwolnienia substancji niebezpiecznych.
		Incydent dotyczący organów	Niedostępność portu bądź ograniczona dostępność portu.

		zarządzających portami.	
		Incydent dotyczący podmiotów prowadzących na terenie portu działalność wspomagającą transport morski.	Niedostępność usługi niezbędnej dla funkcjonowania portu lub ograniczona dostępność usługi.
		Incydent dotyczący VTS (Służba Kontroli Ruchu Statków).	Uszkodzenie systemów informacyjnych kluczowych dla prawidłowego funkcjonowania służby VTS.
	Transport drogowy	Incydent dotyczący zarządzania drogami.	1. Wypadek drogowy, awaria sygnalizacji świetlnej lub awaria innych urządzeń służących do informowania uczestników ruchu drogowego, w wyniku których liczba ofiar i rannych przekracza 11 osób. 2. Wypadek z udziałem co najmniej jednego pojazdu samochodowego transportującego towary niebezpieczne, w wyniku którego doszło do uwolnienia substancji niebezpiecznych.
		Incydent dotyczący Inteligentnych systemów transportowych.	1. Wypadek drogowy, awaria sygnalizacji świetlnej lub awaria innych urządzeń służących do informowania uczestników ruchu drogowego, w wyniku których liczba ofiar i rannych przekracza 11 osób. 2. Wypadek z udziałem co najmniej jednego pojazdu samochodowego transportującego towary niebezpieczne, w wyniku którego doszło do uwolnienia substancji niebezpiecznych.
Bankowość i infrastruktura rynków finansowych		Incydent dotyczący funkcjonowania banków, instytucji kredytowych i infrastruktury rynków finansowych.	1. Wiedza o incydencie jest powszechnie dostępna lub mógł on spowodować istotną szkodę wizerunkową. 2. Szacowany finansowy wpływ incydentu przekracza 5 mln EUR. 3. Incydent rozprzestrzenia się wewnętrznie aż do poziomu członka zarządu odpowiedzialnego za obszar IT (bądź równoważnego stanowiska

			kierowniczego). 4. Incydent będzie prowadzić do naruszenia interesów osób trzecich. 5. Incydent doprowadził do uruchomienia procedur zarządzania kryzysowego. 6. Incydent został zgłoszony do właściwego CSIRT lub Policji.
		Incydent dotyczący transakcji.	Incydent obejmuje 25% płatności realizowanych przez dostawcę usług płatniczych (pod względem liczby transakcji) lub 5 mln EUR.
		Incydent dotyczący użytkowników usług płatniczych.	Incydent obejmuje 50 000 użytkowników lub 25% płatności realizowanych przez użytkowników.
Ochrona zdrowia		Incydent dotyczący zabezpieczenia dostępu, planowania, rozliczania świadczeń opieki zdrowotnej.	1. Incydent doprowadził do braku dostępności usługi powyżej 24 godzin. 2. Incydent doprowadził do braku poufności danych przetwarzanych w usłudze. 3. Incydent doprowadził do braku integralności danych przetwarzanych w usłudze powyżej 24 godzin.
		Incydent dotyczący udzielania świadczenia opieki zdrowotnej przez podmioty lecznicze.	Incydent spowodował ryzyko dla zdrowia lub życia ludzi lub gdy incydent doprowadził do braku poufności danych przetwarzanych w usłudze.
		Incydent dotyczący zaopatrzenia w krew.	Incydent spowodował ryzyko dla zdrowia lub życia ludzi lub incydent doprowadził do braku poufności danych przetwarzanych w usłudze.
		Incydent dotyczący przekazania danych epidemiologicznych.	1. Incydent doprowadził do braku dostępności usługi powyżej 24 godzin. 2. Incydent doprowadził do braku poufności danych przetwarzanych w usłudze. 3. Incydent doprowadził do braku integralności danych przetwarzanych w usłudze.
		Incydent dotyczący gromadzenia i udostępniania Elektronicznej Dokumentacji Medycznej.	1. Incydent doprowadził do braku dostępności usługi powyżej 1 godziny. 2. Incydent doprowadził do braku poufności danych przetwarzanych w usłudze. 3. Incydent doprowadził do braku integralności danych przetwarzanych w usłudze.

		Incydent dotyczący produkcji, obrotu, dystrybucji produktów leczniczych.	Incydent spowodował ryzyko dla zdrowia lub życia ludzi lub Incydent doprowadził do braku poufności danych przetwarzanych w usłudze.
		Incydent dotyczący dostępu do Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego.	1. Incydent spowodował ryzyko dla zdrowia lub życia ludzi. 2. Incydent doprowadził do braku poufności danych przetwarzanych w usłudze. 3. Incydent doprowadził do braku integralności danych przetwarzanych w usłudze.
Zaopatrzenie w wodę pitną i jej dystrybucja		Incydent dotyczący poboru wody.	1. Incydent doprowadził do braku dostępności usługi dla co najmniej 100 000 użytkowników w czasie 8 godzin. 2. Incydent spowodował ryzyko dla zdrowia lub życia ludzi.
		Incydent dotyczący uzdatniania wody.	1. Incydent doprowadził do braku dostępności usługi dla co najmniej 100 000 użytkowników w czasie 8 godzin. 2. Incydent spowodował ryzyko dla zdrowia lub życia ludzi
		Incydent dotyczący dostarczania wody.	1. Incydent doprowadził do braku dostępności usługi dla co najmniej 100 000 użytkowników w czasie 8 godzin. 2. Incydent spowodował ryzyko dla zdrowia lub życia ludzi.
		Incydent dotyczący odprowadzania ścieków.	Incydent doprowadził do braku dostępności usługi dla co najmniej 100 000 użytkowników w czasie 8 godzin.
		Incydent dotyczący oczyszczania ścieków.	Incydent spowodował ryzyko dla zdrowia lub życia ludzi lub poważne zanieczyszczenie środowiska.
Infrastruktura cyfrowa		Incydent dotyczący prowadzenia punktu wymiany ruchu internetowego (IXP) w Polsce.	1. Incydent doprowadził do braku dostępności usługi. 2. Incydent doprowadził do braku poufności usługi. 3. Incydent doprowadził do braku integralności usługi.
		Incydent dotyczący prowadzenia autorytatywnego serwera DNS.	1. Incydent doprowadził do braku dostępności usługi. 2. Incydent doprowadził do braku poufności usługi. 3. Incydent doprowadził do braku integralności usługi.
		Incydent dotyczący prowadzenia rejestru domeny najwyższego	1. Incydent doprowadził do braku dostępności usługi. 2. Incydent doprowadził do braku

		poziomu (TLD).	poufności usługi. 3. Incydent doprowadził do braku integralności usługi.

UZASADNIENIE

Projektowane rozporządzenie stanowi wykonanie upoważnienia ustawowego zawartego w art. 11 ust. 4 ustawy z dnia…… 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …), zwanej dalej „ustawą" i określa progi uznania incydentu za poważny w odniesieniu do usługi kluczowej świadczonej przez operatora usługi kluczowej. Progi określane są według rodzaju zdarzenia w poszczególnych sektorach i podsektorach określonych w załączniku nr 1 do ustawy.

Przedmiotowy projekt rozporządzenia w zakresie swojej regulacji wdraża do polskiego porządku prawnego dyrektywę 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).

Rozporządzenie będzie wykorzystywane przez operatorów usług kluczowych w procesie zgłaszania i obsługi incydentu. Operatorzy usług kluczowych identyfikując incydent i rejestrując go, będą dokonywali klasyfikacji incydentu na podstawie progów uznawania incydentu za poważny. Progi, w zależności od rodzaju zdarzenia, określają liczbę użytkowników, których dotyczy zakłócenie świadczenia usługi kluczowej, czas trwania oddziaływania incydentu na świadczoną usługę kluczową, zasięg geograficzny związany z obszarem, którego dotyczy incydent lub inne czynniki charakterystyczne dla danego sektora lub podsektora.

Progi zostały opracowane w oparciu o propozycje organów właściwych w poszczególnych sektorach. Rozporządzenie określa rodzaj zdarzenia i progi powodujące uznanie incydentu za poważny. Klasyfikacja incydentu jest elementem procesu obsługi incydentu wykonywanego przez operatorów usług kluczowych w oparciu o najlepsze praktyki z zakresu cyberbezpieczeństwa Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji (ENISA), oraz sektorowe wytyczne dotyczące zgłaszania incydentów, opracowywane zgodnie z ustawą przez organy właściwe we współpracy z CSIRT poziomu krajowego.

Przy określaniu progów brano pod uwagę m.in. najlepsze międzynarodowe praktyki prezentowane w materiałach Grupy Współpracy ustanowionej na mocy 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.

Rozporządzenie wejdzie w życie z dniem …….. 2018 r.

Projekt rozporządzenia nie jest sprzeczny z prawem Unii Europejskiej.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projektowana regulacja nie będzie wymagała notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2018 r. poz. 362).

Projekt nie wymaga przedłożenia instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Wejście w życie rozporządzenia nie będzie miało wpływu na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców.

Projekt został udostępniony na stronie Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny” oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra 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).

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie progów uznania incydentu za poważny **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Karol Okoński, Podsekretarz Stanu w Ministerstwie Cyfryzacji **Kontakt do opiekuna merytorycznego projektu** Jakub Dysarz, Departament Cyberbezpieczeństwa, tel. (22) 245 58 38, e-mail:jakub.dysarz@mc.gov.pl	**Data sporządzenia** 30 maja 2018 r. **Źródło:** Prawo UE Upoważnienie ustawowe - art. 11 ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa **Nr w wykazie prac legislacyjnych RM: RC38**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Na mocy ustawy o krajowym systemie cyberbezpieczeństwa, wdrażającej do polskiego porządku prawnego dyrektywę 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), zwaną dalej „dyrektywą 2016/1148/UE", operatorzy usług kluczowych będą zobowiązani do identyfikacji incydentu, jego rejestracji oraz klasyfikacji na podstawie progów uznawania incydentu za poważny. Klasyfikacja incydentu jest elementem procesu obsługi incydentu wykonywanego przez operatorów usług kluczowych w oparciu o najlepsze praktyki z zakresu cyberbezpieczeństwa Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji (ENISA), oraz sektorowe wytyczne dotyczące zgłaszania incydentów, opracowywane zgodnie z ustawą przez organy właściwe we współpracy z CSIRT poziomu krajowego.

Ze względu na powyższe w art. 11 ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa zawarto upoważnienie ustawowe do wydania rozporządzenia w sprawie progów uznania incydentu za poważny. Progi pozwolą na oddzielenie incydentów poważnych od tych, które operatorzy usług kluczowych powinni obsłużyć we własnym zakresie, bez konieczności zgłaszania ich do właściwego CSIRT.

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

Wydanie rozporządzenia określającego progi uznania incydentu za poważny, które w zakresie swojej regulacji wdraża do polskiego porządku prawnego dyrektywę 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.

Rozporządzenie określa rodzaj zdarzenia i progi powodujące uznanie incydentu za poważny. Progi są opracowane w oparciu o propozycje organów właściwych w poszczególnych sektorach lub podsektorach określonych w załączniku nr 1 do ustawy.

Progi, w zależności od rodzaju zdarzenia, określają liczbę użytkowników, których dotyczy zakłócenie świadczenia usługi kluczowej, czas trwania oddziaływania incydentu na świadczoną usługę kluczową, zasięg geograficzny związany z obszarem, którego dotyczy incydent lub inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują.

Określenie progów w poszczególnych sektorach lub podsektorach umożliwi sprawną klasyfikację incydentów przez operatorów usług kluczowych.

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

Ustawa o krajowym systemie cyberbezpieczeństwa stanowiąca implementację dyrektywy 2016/1148/UE, jest w trakcie transpozycji w innych państwach członkowskich UE, podobnie jak i akty wykonawcze do ustawy implementujące dyrektywę 2016/1148/UE.

Za dokument referencyjny dla przedstawienia rozwiązań w innych państwach UE uznać można projekt opracowania przygotowanego w ramach prac grupy roboczej utworzonej decyzją Grupy Współpracy (instytucja utworzona na mocy dyrektywy 2016/1148/UE, w jej skład wchodzą przedstawiciele państw członkowskich) – "Reference document on Incident Notification for Operators of Essential Services" i załączników. Dokumenty te przedstawiają propozycje i rekomendacje dot. wyznaczania progów dla incydentów dotyczących sektorów i podsektorów wymienionych w załączniku nr 2 do dyrektywy 2016/1148/UE oraz odpowiadającemu mu załącznikowi nr 1 do ustawy o krajowym systemie cyberbezpieczeństwa: energia elektryczna, ropa naftowa i gaz, transport kolejowy, transport wodny, transport drogowy, bankowość i infrastruktura rynków finansowych, ochrona zdrowia, zaopatrzenie w wodę pitną i jej dystrybucja, infrastruktura cyfrowa).

Większość państw członkowskich wciąż prowadzi prace nad krajowymi przepisami wdrażającymi dyrektywę 2016/1148/UE.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Operatorzy usług kluczowych w sektorze energii w podsektorze wydobywania kopalin	24	Szacunki oparte na załączniku do projektu ustawy oraz danych URE (trzy podmioty prowadzące kopalnie węgla brunatnego, dwadzieścia podmiotów prowadzących kopalnie węgla kamiennego, jeden podmiot prowadzący kopalnię miedzi)	Wyznaczeni operatorzy usług kluczowych będą zobowiązani klasyfikować i zgłaszać incydenty poważne na podstawie progów określonych rozporządzeniu.
Operatorzy usług kluczowych w sektorze energii w podsektorze energii elektrycznej	30	Szacunki oparte na załączniku do projektu ustawy oraz danych URE (pięć największych podmiotów wytwarzających prąd, OSP, pięciu największych OSD dla gospodarstw domowych, dziewięciu największych OSD dla przedsiębiorców, pięciu największych sprzedawców prądu)	
Operatorzy usług kluczowych w sektorze energii w podsektorze	3	Szacunki oparte na załączniku do projektu ustawy oraz danych	

ciepła		URE (trzy podmioty prowadzące elektrociepłownie, nieobjęte podsektorem energia elektryczna)	
Operatorzy usług kluczowych w sektorze energii 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)	
Operatorzy usług kluczowych w sektorze energii w podsektorze gazu	22	Szacunki oparte na załączniku do projektu ustawy oraz 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)	
Operatorzy usług kluczowych w sektorze energii w zakresie dostaw i usług dla sektora energii oraz jednostki nadzorowane i podległe ministrowi właściwemu do spraw energii oraz ministrowi właściwemu do spraw gospodarki złożami kopalin	15	Dane za BIP Ministra Energii: dwanaście instytutów badawczych, Zakład Unieszkodliwiania Odpadów Promieniotwórczych, Agencja Rezerw Materiałowych i Prezes Wyższego Urzędu Górniczego	
Operatorzy usług kluczowych w sektorze transportu w podsektorze transportu lotniczego	28	Szacunki oparte na załączniku do projektu ustawy oraz danych ULC (czterech przewoźników lotniczych, zarządzający ośmioma największymi portami lotniczymi, piętnaście podmiotów	

		obsługujących urządzenia pomocnicze znajdujące się w portach lotniczych oraz służba kontroli ruchu lotniczego)	
Operatorzy usług kluczowych 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).	
Operatorzy usług kluczowych w sektorze transportu w podsektorze transportu wodnego (dotyczącym transportu morskiego)	21	Szacunki oparte na załączniku do projektu ustawy oraz danych MGMiŻŚ (założono objęcie dziesięciu największych armatorów, ośmiu portów morskich oraz trzech operatorów VTS)	
Operatorzy usług kluczowych w sektorze transportu w podsektorze transportu wodnego (dotyczącym transportu śródlądowego)	0	Informacje z MGMiŻŚ.	
Operatorzy usług kluczowych w sektorze transportu w podsektorze transportu drogowego	24	Szacunki oparte na załączniku do projektu ustawy oraz danych MI (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.	
Operatorzy usług kluczowych w sektorze bankowości i infrastruktury rynków finansowych	67	Szacunki oparte na załączniku do projektu ustawy oraz danych KNF (dwadzieścia największych banków, dziesięć największych banków spółdzielczych, dziesięć największych SKOK, dziesięć największych krajowych zakładów ubezpieczeń, dziesięć największych instytucji płatniczych, dwa banki państwowe, jedna giełda, PWPW, dwaj operatorzy systemu obrotu i jeden kontrahent centralny).	
Operatorzy usług kluczowych w sektorze zaopatrzenia w wodę pitną i jej dystrybucję	31	Przedsiębiorstwa wodno-kanalizacyjne na podstawie danych RCB dotyczących infrastruktury krytycznej.	
Operatorzy usług kluczowych w sektorze ochrony zdrowia	253	Szacunki oparte na danych z rejestrów Głównego Inspektora Farmaceutycznego, CSIOZ i MZ. Wyjaśnienie: Na potrzeby szacunków poczyniono następujące założenia. Uznano, że operatorami usług kluczowych będą podmioty lecznicze (podmioty realizujące świadczenia szpitalne), które miały więcej niż 18 000 hospitalizacji rocznie. Odpowiednio dla województw jest to: 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. Pozostałe podmioty, które spełniały wymogi z załącznika, to NFZ, CSIOZ, pięćdziesięciu największych podmiotów prowadzących hurtownie farmaceutyczne, pięćdziesiąt największych podmiotów prowadzących największe apteki oraz dwudziestu największych wytwórców, importerów lub dystrybutorów substancji czynnych. Uszczegółowienie powyższych danych, w tym doprecyzowanie informacji w zakresie faktycznej liczby podmiotów objętych niniejszą regulacją zostanie dokonane w treści uzasadnień do projektów rozporządzeń wykonawczych do ustawy definiujących progi istotności incydentu oraz wykazu usług kluczowych.	
Operatorzy usług kluczowych w sektorze infrastruktury cyfrowej	8	Szacunki oparte na analizie informacji rynkowych	
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).
Projekt rozporządzenia będzie przedmiotem konsultacji publicznych, opiniowania i uzgodnień międzyresortowych.
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 rozporządzenia 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 2018 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	-	-	-	-	-	-	-	-	-	-	-	-
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Fundusz Ubezpieczeń Społecznych												
Fundusz Pracy												
Narodowy Fundusz Zdrowia												
Wydatki ogółem	-	-	-	-	-	-	-	-	-	-	-	-
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem	-	-	-	-	-	-	-	-	-	-	-	-
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Fundusz Ubezpieczeń Społecznych												
Fundusz Pracy												
Narodowy Fundusz Zdrowia												

Źródła finansowania	Rozporządzenie nie generuje obciążeń finansowych dla sektora finansów publicznych.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Nie dotyczy.

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	Brak wpływu	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	Brak wpływu	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	Brak wpływu	0	0	0	0	0	0
W ujęciu niepieniężnym	duże przedsiębiorstwa	Brak wpływu	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	Brak wpływu	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	Brak wpływu	0	0	0	0	0	0
Niemierzalne	(dodaj/usuń)	Brak wpływu	0	0	0	0	0	0
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Projekt rozporządzenia nie ma wpływu na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na sytuację ekonomiczną i społeczną rodziny, osób niepełnosprawnych oraz osób starszych, a także na obywateli i gospodarstwa domowe.							

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

9. Wpływ na rynek pracy		
Projekt rozporządzenia nie ma wpływu na rynek pracy.		
10. Wpływ na pozostałe obszary		
☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☐ informatyzacja ☐ zdrowie
Omówienie wpływu	Nie dotyczy.	
11. Planowane wykonanie przepisów aktu prawnego		
Projektowane rozporządzenie wejdzie w życie z dniem……2018 r.		
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?		
Nie dotyczy.		
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)		
Brak załączników.		