Warszawa, dnia 16 listopada 2017 r.

RADA DO SPRAW CYFRYZACJI

BM-WOP.002.25.2017

Pani
Anna Streżyńska
Minister Cyfryzacji

Dot. pisma z dn. 31 października br., sygn. DP-III.0211.16.2017

Szanowna Pani Minister,

poniżej przedstawiam uwagi Rady do Spraw Cyfryzacji do ***projektu ustawy o krajowym systemie cyberbezpieczeństwa.***

UWAGI OGÓLNE

Certyfikacja podmiotów świadczących usługi z zakresu cyberbezpieczeństwa

Wskazane w art. 4 pkt 15 projektu ustawy „podmioty świadczące usługi z zakresu cyberbezpieczeństwa", które zostały objęte krajowym systemem cyberbezpieczeństwa, powinny być poddane certyfikacji ABW lub SKW (co najmniej mechanizm analogiczny do nadania certyfikatu bezpieczeństwa teleinformatycznego - zgodnie z art. 50 ust. 3 ustawy o ochronie informacji niejawnych). Z uwagi na zakres zadań w obszarze cyberbezpieczeństwa operatorów usług kluczowych, który może być przekazany ww. podmiotom (art. 15 ust 2 w związku z art. 10 ust. 2, art. 11 ust. 1, art. 12 ust. 1 oraz art. 14), m.in. zbieranie informacji o zagrożeniach, zarządzanie incydentami, zarządzanie ryzykiem, objęcie monitoringiem świadczenie usług kluczowych oraz dostawców usług cyfrowych (art. 23), jak i zadania z zakresu współpracy z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań (art. 35 ust. 5) oraz dostęp do systemu teleinformatycznego, o którym mowa w art. 42 (art. 42 ust. 1 pkt 1), konieczne jest, aby ustawa w sposób literalny odnosiła się do wymogu certyfikacji podmiotów świadczących usługi z zakresu cyberbezpieczeństwa. W tym aspekcie, nadzór ministra właściwego ds. informatyzacji przewidziany w art. 47 ust. 1

pkt. 1 projektu ustawy, należy uznać za model niewystarczający zarówno w kontekście ograniczonych kryteriów kontroli (zawężonych do czynników wskazanych w art. 15 ust. 2), następczego charakteru realizacji przedmiotowej kompetencji, jak i ograniczonego zakresu czynności kontrolnych (zgodnie z procedurą kontroli działalności gospodarczej przedsiębiorcy opisaną w ustawie o swobodzie działalności gospodarczej - art. 48 ust. 1 w związku z art. 47 ust. 1 pkt 1 projektu ustawy).

Potrzeba literalnego ustanowienia mechanizmu certyfikacji podmiotów świadczących usługi z zakresu cyberbezpieczeństwa, które wchodzą w skład krajowego systemu cyberbezpieczeństwa wynika zarówno z okoliczności faktycznych, dokumentów programowych Ministerstwa Cyfryzacji oraz generalnego postulatu jasności prawa (kompleksowości tekstu prawnego). Po pierwsze, z uwagi na podstawowe interesy bezpieczeństwa państwa, certyfikacja ABW zminimalizuje ryzyko wykorzystywania w ramach ochrony teleinformatycznej operatorów usług kluczowych (oraz pozostałych wskazanych powyżej sferach) rozwiązań, które przyczyniałyby się do obniżenia poziomu cyberbezpieczeństwa poprzez m.in. użytkowanie oprogramowania zawierającego celowo umieszczone luki (m.in. *backdoor*). Postulat udziału ABW w procesie weryfikacji producentów i usługodawców rozwiązań w ramach sieci teleinformatycznych organów administracji państwowej, podnoszony był również w *Założeniach strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej* z 2016 roku. Literalne odniesienie wprost do ustawy o ochronie informacji niejawnych, pozwoli także zniwelować ewentualną niejasność co do stosowania właściwych przepisów w kontekście czynności realizowanych przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa, które wchodzą w skład krajowego systemu cyberbezpieczeństwa. Umożliwi to zdjęcie z operatorów usług kluczowych obowiązku każdorazowej wykładni przepisów dotyczących informacji niejawnych w kontekście realizacji poszczególnych zadań i obowiązków przewidzianych w projekcie ustawy przy pomocy podmiotów świadczących usługi z zakresu cyberbezpieczeństwa, co z kolei będzie miało pozytywny wpływ na stopień faktycznej ich realizacji – a zatem odporności krajowego systemu cyberbezpieczeństwa.

Podział zakresu odpowiedzialności za cyberbezpieczeństwo Państwa między 3 odrębne podmioty

Przyjęty w projekcie ustawy ogólny kierunek podziału zakresu odpowiedzialności za cyberbezpieczeństwo Państwa między 3 odrębne podmioty jest nieracjonalny, komplikuje wytyczenie obszarów kompetencyjnych oraz znacząco pogarsza przepływ informacji i skuteczność zarządzania cyberbezpieczeństwem.

Konsekwencją takiej koncepcji, jest konieczność wniesienia do ustawy całego rozdziału regulującego relacje i współpracę między poszczególnymi Centrami, a także przeniesienie części odpowiedzialności i czynności nadzorczych do branżowych ministrów.

Z punktu widzenia podmiotów podlegających regulacjom, taka struktura powoduje dodatkowe komplikacje w postaci założonych w projekcie ustawy równoległych i niezależnych działań kontrolnych wszystkich uprawnionych podmiotów – poszczególnych Centrów oraz właściwych ministrów.

Przyjęcie rozwiązania w postaci jednego centralnego podmiotu realizującego wszystkie wymagane zadania, nie tylko uprości cały system pozwalając przenieść większość szczegółowych regulacji na poziom statutu bądź regulaminu tego podmiotu.

Przede wszystkim nie będzie powodować wzajemnej rywalizacji, sporów kompetencyjnych czy wręcz braku współpracy w poszczególnych obszarach regulowanej materii.

UWAGI DO KONKRETNYCH PRZEPISÓW

Uwagi Rady do Spraw Cyfryzacji do poszczególnych przepisów projektu ustawy o krajowym systemie cyberbezpieczeństwa ujęte zostały w załączonej tabeli.

W imieniu Rady do Spraw Cyfryzacji

Izabela Albrycht
Przewodnicząca Rady
/podpisano elektronicznie/

ARTYKUŁ	UWAGA
Art 1 ust. 1 pkt 1-4	Niezrozumiałe jest zachowanie skrótów od nazwy angielskiej CSIRT (*Computer Security Incident Response Team*); czy nie jest to w kolizji z ustawą **o języku polskim** z dnia 7 października 1999 r.?
Art. 2	1. Brak definicji Incydent Bezpieczeństwa Komputerowego - w ramach którego rozróżnione zostaną systemy IT od systemów OT (technologicznych) ; 2. Brak definicji systemu IT i OT /Brak jasnego zdefiniowania zakresu cyberbezpieczeństwa, który zmienia się ze względu na implementację rozporządzenia NIS w tym dokumencie, powoduje, że podmioty będące adresatem tej ustawy nie będą w 100% pewne zakresu ochrony usług i procesów, szczególnie, że definiuje się systemy informatyczne, które inaczej są nazywane w świecie IT a inaczej w świecie sieci technologicznych. Przykładem może tu być branża energetyczna, gdzie w przypadku systemów i sieci technologicznych mówi się o „łączności" i „systemach SCADA. Należy pamiętać, że będzie to pierwsze poważne zderzenie świata z unormowanymi i ustandaryzowanymi protokołami ze światem, gdzie prawie każdy z liczących się producentów automatyki i systemów do sterowania sieciami technologicznymi „stworzył" swój własny protokół transmisyjny/
Art. 2 pkt 5	„Dany poziom zaufania" - w ustawie nie definiuje się co oznacza dany poziom zaufania. Nie ma też odniesienia do definicji, która byłaby w innych dokumentach. Brak takiego zapisu może nie być istotną przeszkodą w działaniu ustawy, ale pozwala na różną interpretacją czy dane procesy wymagają dbałości w obszarze cyberbezpieczeństwa, czy też nie. Elastyczność w określaniu „danego poziomu zaufania", może być wykorzystane do bagatelizowania kwestii zaistniałych incydentów poprzez np. nieklasyfikowanie zdarzenia do incydentu zwykłego (Art. 2.11) a przez to innych incydentów.

Art. 2 pkt 8-12	W przedstawionym projekcie występuje niejaki „mętlik” definicyjny, który może poważnie rzutować na stosowanie tej ustawy w praktyce. Chodzi o definicję zasadniczego pojęcia, jakim jest „incydent”. Z podanych w art. 2. definicji wynika, że: 1. Pojęcie to obejmuje różne kategorie incydentów: **K**rytyczny **P**oważny **I**stotny **Z**wykły 2. Mają miejsce następujące relacje: **K** jest zawarte w **P** **K** jest zawarte w **I** **K** jest zawarte w **Z** 3. Dalej: **P** jest zawarte w **Z** 4. Natomiast **Z** jest definiowane jako dowolne zdarzenie o niekorzystnym wpływie na cyberbezpieczeństwo. 5. Dodatkowo **I** jest definiowane przez odniesienie do dokumentu zawierającego odnośną decyzję Komisji Europejskiej. Przy tak sformułowanych definicjach można postawić szereg pytań, na które nie ma jednoznacznej odpowie-

	dzi, np.: Czy incydent typu **I** jest również incydentem typu **Z**? Czy incydent typu **P** jest również incydentem typu **I**? Czy Ustawa celowo dopuszcza możliwość, że incydent istotny (typu **I**) może nie być ani **Z**wykły, ani **P**oważny, ani **K**rytyczny? Taki stan definicyjny może przysporzyć wielu kłopotów, np. w zakresie ustalania, kto jest za co odpowiedzialny i czego dotyczą przepisy szczegółowe tej ustawy. „Incydent krytyczny, poważny, istotny albo zwykły"– definicje incydentów są nieprecyzyjne co może skutkować trudnościami w klasyfikacji przez podmioty podlegające ustawie, w szczególności przedsiębiorców. Niektóre z parametrów służących do zdefiniowania kategorii incydentu są niemierzalne lub też mierzalne dopiero po zdarzeniu w sposób statystyczny np. „zaufanie do instytucji publicznych". Podmiot komercyjny będzie mieć problem z klasyfikacją zdarzenia. Wydaje się że w takiej formie dopiero po zakończeniu trwania incydentu będzie możliwe w sposób jednoznaczny (ale być może negocjacyjny) określenie jego przyporządkowania. Zbyt szeroka jest definicja „incydentu zwykłego" - przykładowo: każde wydarzenie prowadzące do ujawnienia informacji związanych z systemem informatycznym lub hierarchią władzy w jednostce może mieć niekorzystny wpływ na cyberbezpieczeństwo.
Art. 2 pkt 22	RdC sugeruje uproszczenie definicji wyszukiwarki internetowej przez zastąpienie określenia „wyszukiwanie wszystkich stron internetowych lub stron internetowych w danym języku za pomocą zapytania przez podanie" określeniem „wyszukiwanie publicznie dostępnych stron internetowych"

Art. 4	W ustawie brakuje jasno określonego stałego organu koordynacyjno – kontrolnego w zakresie nadzoru nad efektywnością pracy zespołów CSIRT i pozostałych elementów Krajowego Systemu Cyberbezpieczeństwa, który na poziomie KRM w sposób stały koordynowałby system.
Art. 4 pkt 12	W przypadku samorządów, ustawa (odmiennie niż w pkt 11 dla administracji rządowej) nie obejmuje jednostek podległych. Część z nich stanowi elementy infrastruktury krytycznej (np. woda).
Rozdział 2	Ustawodawca „zgubił" podmioty, które jako spółki samorządowe lub podmioty – spółki prawa handlowego funkcjonują w obszarze samorządowym i są operatorami usług kluczowych – np. gminne spółki wodno-kanalizacyjne, elektrociepłownie. Należy uszczegółowić zakres operatorów usług kluczowych w zakresie struktur samorządowych.
Art. 5 ust. 2, 4 i 5	„Decyzja i konsekwencje określenia, że dany podmiot jest operatorem usługi kluczowej" – decyzja taka ma wpływ na prowadzoną działalność gospodarczą, a więc po wydaniu decyzji powinien być czas na dostosowanie jej działalności z ewentualną zmianą modelu biznesowego związanego z tą usługą. Z zapisów ustawy wynika natychmiastowe żądanie wykonalności (Art. 5. punkt 5), co może powodować problem z realizacją wymogów nałożonych w ustawie.
Art. 7 ust. 3	„Niejawność Progów istotności skutku zakłócającego" - wydaje się że progi istotności powinny być jawne, będąc częścią legislacji w zakresie cyberbezpieczeństwa. Niejawność może powodować ograniczenie liczby podmiotów decydujących się na działanie w obszarach biznesowych wymienionych w załączniku do uchwały, gdyż firmy te nie będą mogły ocenić wpływu legislacji na planowany model biznesowy i plan biznesowy. Przemyślana pod kątem cyberbezpieczeństwa decyzja związana z wejściem w działalność w danym obszarze, pozwoli na wcześniejsze uniknięcie problemów związanych z potencjalną nieprofesjonalną działalnością nowego podmiotu.

Art. 8 ust. 6	Wykaz podmiotów uprawnionych do uzyskania informacji z wykazu operatorów usług kluczowych, pokazuje że nie może tej informacji uzyskać organ samorządu terytorialnego, którego podmiot zostanie wpisany na listę. Konsekwencją jest fakt, że prezes spółki/szef podmiotu **nie może nawet poinformować** burmistrza o tym fakcie i wynikających z tego obowiązkach. „Udostępnianie informacji o wykazie operatorów usług kluczowych" - informacje te powinny być udostępniane oprócz wymienionych także wszystkim podmiotom wchodzącym w skład krajowego systemu cyberbezpieczeństwa. Dzięki tej informacji podmioty te mogą świadomie podejmować decyzje o wyborze partnera biznesowego, co może przekładać się na świadczoną usługę końcową.
Art. 10 ust. 2 pkt 1	Konieczne jasne i konkretne podanie, że dotyczy to zarówno sieci IT jak i OT (technologicznych) - jeżeli takie istnieją, inaczej będzie to ustawa rozwiązująca problem częściowo – w tym zakresie należy bardziej uszczegółowić zakres procesów i usług jakie będą objęte regulacją już na poziomie ustawy ze względu na istotę problemu.
Art. 10 ust. 2 pkt 2	Czy CSIRT będą mieć specjalistów od analizy wszystkich incydentów - trzeba pamiętać, że ile technologii produkcyjnych tyle protokołów na świecie, co oznacza, że nie ma standaryzacji protokołów transmisyjnych w sieciach technologicznych – sugeruje się utworzenie pojęcia CERT'ów sektorowych specjalizujących się w technologiach sieci produkcyjnych
Art. 10 ust. 2 pkt 3	Odpowiednie i proporcjonalne środki techniczne, a w Ocenach Skutków Regulacji zakłada się : - 5-10 tys na pracownika SOC - Koszt SOC - 1 mln - Audyt 50 tys To nie są koszty realne i proporcjonalne. Dlatego też sugeruje się utworzenie CERT'ów sektorowych i sugero-

	wanie operatorom usług kluczowych oraz CERT'om sektorowym wykorzystywanie specjalistycznych narzędzi audytowych do sieci technologicznych i do stałego monitorowania tych sieci.
Art. 11	„Opracowanie dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych używanych do świadczenia usług kluczowych". Wydaje się że czas 6 miesięcy może być trudny dla podmiotów które dopiero rozpoczną dostosowywanie się do zapisów uchwały po decyzji, iż jest on operatorem usługi kluczowej. W takim przypadku czas ten z realnych powodów działania rynku (zatrudnienie specjalistów, opracowanie procesów itp.) może być nierealny.
Art. 12 ust. 3 i 4 oraz art. 13 ust. 1	Artykuł 12 ust. 3, ust. 4 oraz artykuł 13 ust. 1 odwołują się do incydentu poważnego (stopnień niższy niż incydent krytyczny). Artykuł 12 ust. 1 pkt 6 rozróżnia incydent poważny i incydent krytyczny. Czy to pociąga za sobą brak obowiązku zgłaszania incydentu krytycznego?
Art. 15 ust. 1 pkt 2	Zgodnie z art. 15 ust. 1 pkt 2 operatorzy usług kluczowych zobowiązani są do zapewnienia użytkownikowi usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową. Pominąwszy nieprecyzyjny charakter przepisu, warto wskazać, iż jest on również pozbawiony sankcji (art. 57), co w znacznym stopniu może przyczynić się do braku realizacji dyspozycji ustanowionej nim normy. Operatorzy usług kluczowych, jako podmioty realizujące zadania o podstawowym znaczeniu dla funkcjonowania współczesnego społeczeństwa i gospodarki, powinni być zobowiązani do uczestnictwa w budowaniu świadomości użytkowników w obszarze cyberbezpieczeństwa. Warto w tym kontekście rozważyć nałożenie obowiązku przesyłania okresowej informacji (nie tylko „zapewniania dostępu do wiedzy") dotyczącej aktualnych zagrożeń cybernetycznych mogących wiązać się z korzystaniem z danej usługi kluczowej (np. na zasadzie aktualizacji polityki prywatności udostępnianych użytkownikom przez platformy cyfrowe lub działań edukacyjnych). Będzie to też miało korzystny wpływ na cyberbezpieczeństwo operatorów usług kluczowych, którzy mogą dzię-

	ki temu uzyskiwać bieżącą informację od użytkowników na temat wykrytych podatności i incydentów (zidentyfikowanych dzięki ostrzeżeniom operatorów). Warto również rozważyć, aby obowiązek ten dotyczył także innych podmiotów krajowego systemu cyberbezpieczeństwa, np. przedsiębiorstw telekomunikacyjnych (art. 4 pkt 5), organów administracji publicznej (art. 4 pkt 6), jednostek samorządu terytorialnego (art. 4 pkt 12).
Art. 15 ust. 2	Artykuł rodzący wiele pytań i wątpliwości. Czy na pewno każdy operator usługi kluczowej powinien korzystać z usług zewnętrznego podmiotu świadczącego usługi cyberbezpieczeństwa, jeżeli tak to w jakim zakresie i kto określi standardy takiego podmiotu. Uważam, że tego typu podmioty powinny być certyfikowane w swoim zakresie przez CSIRT ABW lub MON lub NASK w zakresie takim, dla jakiego podmiotu usług kluczowych będą świadczyć usługi.
Art. 15 ust. 4	Zdaniem RdC Minister Cyfryzacji nie ma kompetencji aby określać wymagania np. na CERT dla Energetyki albo CERT dla branży zbrojeniowej - to powinien robić CSIRT właściwy dla danego operatora kluczowego.
Art. 16	Ustawa nakłada obowiązek audytu procedur, brakuje obowiązku przeprowadzenia rzeczywistych testów bezpieczeństwa. RdC sugeruje wprowadzenie obowiązku przeprowadzenia co określony czas audytu bezpieczeństwa przez zewnętrznych certyfikowanych pentesterów.
Art. 16 ust. 1	Zgodnie z art. 16 ust. 1 projektu ustawy, operatorzy usług kluczowych są zobowiązani do przeprowadzenia co najmniej raz na dwa lata audytu bezpieczeństwa teleinformatycznego. Z uwagi na bezprecedensową dynamikę rozwoju liczby i zaawansowania zagrożeń w cyberprzestrzeni oraz fundamentalną rolę operatorów usług kluczowych dla funkcjonowania współczesnego społeczeństwa i gospodarki, audyty bezpieczeństwa teleinformatycznego powinny być realizowane co pół roku. Tym samym ustawa powinna doprecyzować procedurę wyboru (prawdopodobnej certyfikacji jak w przypadku

	podmiotów świadczących usługi z zakresu cyberbezpieczeństwa) oraz organ dokonujący akredytacji (art. 16 ust. 2) podmiotów uprawnionych do realizacji audytów.
Art. 16 ust. 2	W projekcie ustawy brakuje informacji o warunkach koniecznych do spełnienia w celu otrzymania odpowiedniej akredytacji oraz o instytucji odpowiedzialnej za przydzielanie takich akredytacji. Problem rodzi zapis „akredytowana jednostka". CO to ma być za akredytacja i jakie wymagania ma spełniać ta jednostka? Problem w tym, że nie ma standaryzacji tych jednostek a dodatkowo ograniczamy się do np. jednostek dużych bądź specjalizowanych typu PwC, Ey, KPMG, wykluczając mniejsze polskie firmy realizujące takie audyty. Dlaczego CSIRT albo CERT sektorowe nie mogą przeprowadzać samodzielnie audytów przy użyciu powszechnie znanych i często dostępnych narzędzi dla tych operatorów?
Rozdział 4	Brakuje możliwości zlecenia zadań związanych z cyberbezpieczeństwem podmiotom zewnętrznym (taką możliwość dostawcom usług elektronicznych daje art. 23). Efektem takiego ograniczenia jest spadek jakości ochrony cybernetycznej lub wzrost jej kosztów.
Rozdział 5	• Znaczna cześć regulacji w tym rozdziale jest konsekwencją przyjętej koncepcji **3 różnych** ośrodków CSIRT. Skutkuje to koniecznością regulowania ich wzajemnych relacji oraz szczegółowego podziału kompetencji. • Przewidziano np. sytuacje zgłoszeń do niewłaściwego CSIRT i przekazywania ich dalej, co wydłuży procedurę. • Niejasne jest forsowanie koncepcji 3 odrębnych struktur, przy jednoczesnym zapisaniu możliwości wzajemnego powierzania sobie zadań – art. 28 ust. 10.

	• Art. 36 uwypukla inny aspekt rozproszenia obszarów kompetencji między 3 ośrodki – w przypadku poważnego incydentu na styku wszystkich ośrodków, **powstaną 3 niezależne analizy** potencjalnych skutków incydentu. • Art. 37 explicite pokazuje niewydolność takiego rozwiązania, ustanawiając strukturę nadrzędna nad trzema CSIRT, o niesprecyzowanych ostro kompetencjach - szczególnie wobec poszczególnych CSIRT; a także rozbudowując procedury uzgadniania stanowisk, decyzji i działań. Jednocześnie proponowane są rozwiązania blokujące, które mogą doprowadzić do paraliżu tego ciała – np. „*Zespół na posiedzeniu: 1)* ***wyznacza jednomyślnie*** *CSIRT koordynujący obsługę incydentu*”.
Art. 42 ust. 13	RdC sugeruje zmianę „mogą być udostępniane” na „są udostępniane na wniosek”.
Art. 42 ust. 14	Dostęp do systemu teleinformatycznego służącego do zgłaszania incydentów powinien być udostępniany każdemu podmiotowi związanemu Ustawą.
Art. 49 pkt 1	„Zapewnienie osobie prowadzącej czynności kontrolne swobodnego wstępu i poruszania się bez przepustki po terenie podmiotu kontrolowanego” – w wielu przypadkach nie wydaje się to realne. W firmach istnieją systemy kontroli dostępu, dodatkowo działanie kontrolowanego podmiotu może dotyczyć branży, w której do samodzielnego poruszania po terenie zakładu, wymagana jest znaczna wiedza i znajomość prowadzonej działalności wraz z przeszkoleniem (np. petrochemia, przedsiębiorstwa energetyczne itp.). Powinno być zapisane, że podmiot kontrolowany zapewni swobodny wstęp, a to w jakiej to zrobi formie (np. pracownik merytoryczny opiekujący się osobą kontrolującą) to kwestia organizacyjna. Prawo do swobodnego poruszania się po kontrolowanym obiekcie jest sprzeczne z podstawowymi wymogami bezpieczeństwa serwerowni.

Art. 50 ust. 1	Konieczne jest wprowadzenie ograniczenia informacji pozyskiwanych na nośnikach cyfrowych do informacji związanych bezpośrednio z bezpieczeństwem danego systemu informatycznego.
Rozdział 10	Projekt ustawy nie zawiera jednoznacznego postanowienia, iż kary pieniężne stanowią dochód budżetu państwa.
Art. 57 ust. 1	1. Problem: **Nieokreślenie sankcji za naruszenie obowiązków wynikających z ustawy przez dostawców usług cyfrowych.** Dyrektywy Parlamentu Europejskiego i Rady (EU) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dalej: Dyrektywa), określa wymagania w zakresie cyberbezpieczeństwa **dotyczące operatorów usług kluczowych i dostawców usług cyfrowych**. Podobnie, przedstawiony projekt ustawy określa zobowiązania operatorów usług kluczowych oraz dostawców usług cyfrowych (rozdział 3). **Zgodnie z art. 21 Dyrektywy, państwa członkowskie zobowiązane są do wprowadzenia sankcji za naruszenie przepisów krajowych implementujących Dyrektywę.** Przepis art. 57 ust. 1 projektu ustawy, reguluje odpowiedzialność operatorów usług kluczowych za naruszenie określonych przepisów ustawy. **Projekt ustawy nie przewiduje jednak sankcji za naruszenie przepisów przez dostawców usług cyfrowych**. Projekt nie przewiduje nakładania kar na dostawców usług cyfrowych. Brak sankcji za niewykonanie przez dostawców usług cyfrowych obowiązków wynikających z ustawy, prowadzić może do nienależytego wykonywania przez takie podmioty obowiązków ustawowych, a w konsekwencji do obniżenia poziomu cyberbezpieczeństwa. Zasadnym wydaje się zatem wprowadzenie sankcji (być może również kar pieniężnych) za naruszenie ustawy przez dostawców usług cyfrowych. 2. Problem: **Niezgodność przepisu art. 47 ust. 2 z przepisami rozdziału X („Przepisy o karach pieniężnych), w tym art. 57 ust. 1 projektu ustawy.**

	Art. 47. *1. Nadzór w zakresie stosowania przepisów ustawy sprawują:* *1) minister właściwy do spraw informatyzacji w zakresie spełniania przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa wymogów, o których mowa w art. 15 ust. 2;* *2) organy właściwe w zakresie:* *a) wykonywania przez operatorów usług kluczowych wynikających z ustawy obowiązków dotyczących przeciwdziałania zagrożeniom cyberbezpieczeństwa i zgłaszania incydentów, związanych ze świadczonymi usługami kluczowymi,* *b)* ***spełniania przez dostawców usług cyfrowych wymogów bezpieczeństwa świadczonych przez nich usług cyfrowych i zgłaszanie incydentów****, zgodnie z decyzją wykonawczą Komisji Europejskiej 2017/…/UE.* *2.* ***W ramach nadzoru, o którym mowa w ust. 1****, organ właściwy lub minister właściwy do spraw informatyzacji:* *1) prowadzi kontrole w zakresie, o którym mowa w ust. 1;* *2) zobowiązuje do usunięcia nieprawidłowości ustalonych w wyniku kontroli;* ***3) nakłada kary pieniężne.*** Zgodnie z przepisem art. 47 ust. 1 pkt 2 lit b) projektu ustawy, właściwy organ sprawuje nadzór nad spełnieniem przez dostawców usług cyfrowych wymogów bezpieczeństwa. Przepis art. 47 ust. 2 pkt. 3 projektu ustawy, przewiduje natomiast, że w ramach takiego nadzoru właściwy organ lub minister ds. Informatyzacji nakłada kary pieniężne. A zatem, **literalne brzmienie przepisu sugeruje, że kary pieniężne mogą zostać nałożone również na dostawców usług cyfrowych** (art. 47 ust. 2 odwołuje się do całego ust. 1, a nie tylko do ust. 1 pkt 2 lit a). Przepisy rozdziału X projektu ustawy (przepisy o karach pieniężnych) nie przewidują natomiast nakładania kar pieniężnych na dostawców usług cyfrowych. Należy zatem, wprowadzić redakcję przepisów nie powodująca tego rodzaju sprzeczności. **3.** Problem: **Niejednoznacznie (lub jak się wydaje zbyt wąsko) opisane okoliczności stanowiące podsta-**

	wę naliczenia kary. a) *Art. 57 ust. 1 pkt 3 projektu ustawy.* Zgodnie z *art. 11 ust. 2 projektu ustawy:* *„Operatorzy usług kluczowych* ***opracowują dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych …”.*** Natomiast art. 11 ust. 3 projektu ustawy, przewiduje wydanie przez Radę Ministrów rozporządzenia określającego „*sposób tworzenia,* ***aktualizacji****, oraz zakres informacji zawartych w dokumentacji (..)*.” Przewiduje się zatem zasady aktualizacji dokumentacji. Zgodnie z art. 57 ust. 1 pkt 3 projektu ustawy, kara pieniężna może zostać nałożona jeżeli operator usług kluczowych „ **nie opracował dokumentacji**”. Przepis nie przewiduje możliwości nałożenia kary w przypadku brak „aktualizacji” dokumentacji. Jeżeli zatem operator usług kluczowych opracuje dokumentacje ale potem zaniecha jej aktualizacji, to nie będzie istnieć podstawa do nałożenia kary (wydaje się, że powinna istnieć realna sankcja również za brak wymaganej aktualizacji dokumentacji). b) *Art. 57 ust. 1 pkt 4 projektu ustawy* Artykuł 12 projektu ustawy przewiduje szereg obowiązków operatora usług kluczowych (6 podpunktów). Przepis art. 57 ust. 1 pkt 4 projektu ustawy, przewiduje karę, jeżeli operator usług kluczowych „nie wykonuje obowiązków wynikających z art. 12 ust. 1”. Powstać może jednak wątpliwość, czy karę można nałożyć wyłącznie w przypadku, w którym operator usług kluczowych nie wykona wszystkich obowiązków opisanych w art. 12 ust. 1 projektu ustawy (a przynajmniej dwóch, bo termin – „obowiązków” użyty został w liczbie mnogiej), czy też karę można nałożyć w przypadku niewykonania, któregokolwiek z obowiązków opisanych w art. 12 ust.1 projektu ustawy. Wydaje się, że niewykonanie któregokolwiek (tj. nawet jednego) z opisanych obowiązków, skutkować powinno możliwością nałożenia kary. c) *Brak kary za naruszenie obowiązku wynikającego z art. 15 ust. 1 pkt 2 projektu ustawy (zapewnienia*

	użytkownikowi usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania ..). Wydaje się, że niewykonanie tego obowiązku również powinno zostać zabezpieczone stancją w postaci kary pieniężnej.
Art. 57 ust. 1 pkt 9	Zdaniem RdC kary są nieadekwatne do rodzaju i zakresu szkód jakie może spowodować nie stosowanie się do zapisów niniejszej ustawy. Straty spowodowane incydentami cyberbezpieczeństwa mogą i będą powodować znaczne straty w mieniu, a ich efekt może spowodować realne zagrożenie dla zdrowia wielu osób /np. awaria instalacji w rafinerii na skutek ataku hakerskiego może spowodować wybuch i nie tylko śmierć osób, ale także skażenie obszaru wokół rafinerii/. RdC sugeruje uzależnienie kar od % obrotu spółek analogicznie do kar w Rozporządzeniu o Ochronie Danych Osobowych, wtedy zachowamy równe obciążenie dla każdej wielkości przedsiębiorstwa. W przypadku samorządów można analogicznie ograniczyć kary po poziomu 100 tys. PLN za pojedyncze naruszenie ale włączyć odpowiedzialność karną zarządzającego jednostką samorządową.
Art. 57 ust. 2	1. Problem – **Zbyt niska wysokość kar pieniężnych.** Przepis art. 21 Dyrektywy nakazuje określenie w przepisach krajowych sankcji za naruszenie przepisów krajowych, przyjętych na podstawie Dyrektywy. **Przepis art. 21 Dyrektywy przewiduje przy tym, że „Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające."** Przepis art. 57 ust. 2 przewiduje kary pieniężne w wysokości od 1 tys do 100 tys zł. Należy zauważyć, że przepis określa maksymalny wymiar kary (co podkreśla się również w uzasadnieniu ustawy). W praktyce, należy liczyć się zatem z wymierzaniem kary na niższym poziomie. RdC uważa, że generalnie dobrym rozwiązaniem jest przyjęty w projekcie ustawy model sankcji w postaci kar pieniężnych. Mając jednak na uwadze, jak istotna dla bezpieczeństwa państwa i obywateli jest kwestia zapewnienia odpowiedniego poziomu cyberbezpieczeństwa, proponowana wysokość kar pieniężnych wydaje się zbyt

	niska. **Wątpliwym jest, czy kary pieniężne w proponowanej wysokości rzeczywiście stanowić będą „skuteczną" i „odstraszającą" sankcje**. Ponadto, ustanowienie maksymalnej wysokości kary pieniężnej, uniemożliwia elastyczne dostosowanie jej do wielkości, pozycji rynkowej i sytuacji gospodarczej podmiotu, który dopuścił się naruszenia (np. kara w wysokości 10 tys. zł może być skuteczna odnośnie „niewielkiego" przedsiębiorcy, a zupełnie niezauważalna dla innego, „większego" przedsiębiorcy). **RdC proponuje wprowadzenie systemu, przewidującego możliwość nałożenia kary w wysokości do określonej w ustawie kwoty lub do określonej wartości procentowej przychodów za poprzedni rok. (tj. kara do X zł lub do X % przychodów za poprzedni rok).** Decydowałby przy tym wartość wyższa. Jak zostało to już wskazane, wydaje się, że kwota pieniężna (tj. kwota X) powinna zostać ustalona na wyższym poziomie niż przewidziana w projekcie ustawy. Proponowane rozwiązanie nie jest nowe w polskim systemie prawnym. Podobne rozwiązanie przewiduje art. 83 Ogólnego rozporządzenia o ochronie danych. Ponadto, system kar pieniężnych kalkulowanych w oparciu o wielkość przychodu przewiduje np. Prawo Telekomunikacyjne z dnia 16 lipca 2004 r. (art. 209 – art. 210), ustawa o ochronie konkurencji i konsumentów (art. 106). Oczywiście dopracowania wymagają kwestie szczegółowe np. czy kara obliczana jest od przychodu/obrotu, za ostanie rok obrotowy/kalendarzowy itp.
Załącznik do ustawy	Podmiotem świadczącym usługi DNS jest prawie każdy dostawca internetu udostępniający swoje systemy rozwiązywania nazw klientom oraz każda kawiarnia udostępniająca swoim klientom bezpłatny dostęp do internetu (każdy router WiFi ma wbudowany serwer DNS).
Uwaga dotycząca wielu artykułów	Opisy incydentów powinny być akceptowane w języku polskim lub angielskim, w szczególności tam, gdzie jednostki zgłaszające korzystają z zagranicznych podmiotów zajmujących się bezpieczeństwem sieci lub zatrudnia-

	ją międzynarodowe zespoły zajmujące się kwestiami cyfrowymi.

Signature Not Verified
Dokument podpisany przez Izabela Albrycht
Data: 2017.11.16 10:16:20 CET