



Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji

Warszawa, dn. 11.06.2018 r.
KIGEiT/989/06/2018

Sz. P. Marek Zagórski
Minister
Ministerstwo Cyfryzacji
ul. Królewska 27
00-060 Warszawa

Dot. prac nad projektem rozporządzenia Rady Ministrów w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych

Działając w imieniu Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji (dalej „Izba” lub „KIGEiT”), odnosząc się do projektu rozporządzenia Rady Ministrów w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych, Izba przedstawia co następuje.

Podkreślenia wymaga, iż najważniejsze uwagi Izby do projektu rozporządzenia dotyczą relacji projektu rozporządzenia do projektu ustawy o krajowym systemie cyberbezpieczeństwa (dalej „projekt ustawy”), w związku z czym uwagi przedstawione w dalszej części pisma odnoszą się również do samego projektu ustawy, w stosunku do której projektowane rozporządzenie ma charakter wykonawczy.

1. Usługi kluczowe powinny zostać zdefiniowane i skatalogowane bezpośrednio w tekście ustawy o krajowym systemie cyberbezpieczeństwa, bez odsyłania do rozporządzenia wykonawczego czy załącznika do ustawy.

Art. 5 ust. 1 projektu ustawy o krajowym systemie cyberbezpieczeństwa stanowi, że *operatorem usługi kluczowej jest podmiot, o którym mowa w załączniku nr 1 do ustawy, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy wydał decyzję o uznaniu za operatora usługi kluczowej. Załącznik nr 1 do ustawy określa sektor, podsektor oraz rodzaj podmiotu. Zgodnie z art. 6 pkt 1 projektu ustawy Rada Ministrów ma określić w drodze rozporządzenia wykaz usług kluczowych, o których mowa w art. 5 ust. 2 pkt 1, kierując się przyporządkowaniem usługi kluczowej do danego sektora, podsektora i rodzaju podmiotu wymienionych w załączniku nr 1 do ustawy oraz znaczeniem usługi dla utrzymania krytycznej działalności społecznej lub gospodarczej. Tym samym poza ustawą znajduje się wykaz usług kluczowych, który ma być określony rozporządzeniem do ustawy.*

W ocenie Izby taka konstrukcja jest niedopuszczalna, gdyż pozwala Radzie Ministrów na dowolne i nieskrępowane poszerzanie o nowe podmioty i przedsiębiorców kręgu podmiotów zobowiązanych do stosowania przepisów ustawy o krajowym systemie cyberbezpieczeństwa, poprzez zmianę rozporządzenia wykonawczego do ustawy.

Ponadto, problem konstrukcyjny dotyczący relacji projektu ustawy do projektu rozporządzenia w sprawie usług kluczowych jest tym bardziej widoczny, jeśli zestawimy informacje zawarte w projekcie załącznika nr 1 do ustawy z projektem rozporządzenia:

- załącznik nr 1 do ustawy określa sektor, podsektor oraz rodzaj podmiotu, który może zostać uznany za operatora usługi kluczowej;
- projekt rozporządzenia w sprawie usług kluczowych określa sektor, podsektor oraz rodzaj podmiotu, który może zostać uznany za operatora usługi kluczowej (a więc te same kategorie, co załącznik nr 1), usługę kluczową oraz próg istotności skutku zakłócającego incydentu dla świadczenia usługi kluczowej.

Zatem w sposób oczywisty treść załącznika nr 1 do ustawy i projektu rozporządzenia w sprawie usług kluczowych dublują się, a relacja załącznika do rozporządzenia jest niejasna i niezrozumiała.

Taka konstrukcja, powodująca dublowanie się przepisów jest tym bardziej nieuzasadniona, że wszystkie postanowienia przewidziane w załączniku i rozporządzeniu w sprawie usług kluczowych (za wyjątkiem ewentualnie progu istotności skutku zakłócającego incydentu dla świadczenia usługi kluczowej, który faktycznie może być przedmiotem regulacji na poziomie rozporządzenia) mogą i powinny zostać zapisane bezpośrednio w treści samej ustawy o krajowym systemie cyberbezpieczeństwa, co dałoby ustawodawcy i społeczeństwu kontrolę nad tym, wobec jakich podmiotów przepisy ustawy znajdują zastosowanie.

Zdefiniowanie i ujęcie bezpośrednio w tekście ustawy o krajowym systemie cyberbezpieczeństwa wykazu usług kluczowych lub operatorów usług kluczowych jest tym bardziej uzasadnione, iż lista „operatorów usług kluczowych” stanowi załącznik II do dyrektywy 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, którą to listę – po wprowadzeniu niezbędnych zmian i dostosowaniu do krajowego porządku prawnego – można przenieść do tekstu ustawy. W praktyce może to polegać na przeniesieniu obecnego brzmienia projektu rozporządzenia w sprawie usług kluczowych bezpośrednio do tekstu projektu ustawy o krajowym systemie cyberbezpieczeństwa. Takie rozwiązanie ma niewątpliwie zalety, takie jak:

- kontrola ustawodawcy i społeczeństwa nad tym, jakie podmioty będą objęte obowiązkami wynikającymi z ustawy o krajowym systemie cyberbezpieczeństwa;
- uchylenie prawnych i praktycznych problemów związanych z niejasną relacją ustawy do rozporządzenia w sprawie usług kluczowych.

Jednocześnie rozwiązanie takie nie obniża elastyczności obecnej konstrukcji, przy założeniu, że załącznik do ustawy miałby podlegać zmianom w tym samym trybie co zmiana ustawy.

2. Wyłączenie stosowania przepisów ustawy o krajowym systemie cyberbezpieczeństwa do przedsiębiorców telekomunikacyjnych a wykaz usług kluczowych przewidzianych w projekcie rozporządzenia w sprawie usług kluczowych.

Art. 1 ust. 2 pkt 1 projektu ustawy o krajowym systemie cyberbezpieczeństwa stanowi wprost, że *ustawy nie stosuje się do przedsiębiorców telekomunikacyjnych, o których mowa w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne [...] w zakresie wymogów*

dotyczących bezpieczeństwa i zgłaszania incydentów. Wyłączenie takie jest w pełni zasadne biorąc pod uwagę, iż obowiązki przedsiębiorców telekomunikacyjnych w zakresie bezpieczeństwa teleinformatycznego zostały szczegółowo i kompleksowo uregulowane w przepisach ustawy Prawo telekomunikacyjne.

Niemniej jednak pojawia się wątpliwość co do tego, jak rozumieć powyższe, zasadne wyłączenie w świetle przepisów projektu rozporządzenia w sprawie usług kluczowych, które do usług kluczowych zalicza m.in.

- a) prowadzenie autorytatywnego serwera DNS;
- b) prowadzenie punktu wymiany ruchu internetowego (IXP);
- c) prowadzenie rejestru domeny najwyższego poziomu (TLD);

W praktyce bowiem usługi wymienione w punktach a) – c) powyżej [a w szczególności a) i b)] mogą być świadczone przez przedsiębiorców mających status przedsiębiorcy telekomunikacyjnego, a sama usługa może być elementem składowym albo towarzyszącym świadczeniu usługi telekomunikacyjnej. Powstaje wątpliwość, czy w takim przypadku wyłączenie przewidziane w art. 1 ust. 2 pkt 1 projektu ustawy o krajowym systemie cyberbezpieczeństwa znajduje zastosowanie – w ocenie Izby również w takim przypadku należy stosować wyłączenie dla przedsiębiorców telekomunikacyjnych przewidziane w projekcie ustawy. Biorąc pod uwagę zakres i kompleksowość obowiązków dotyczących cyberbezpieczeństwa przewidzianych w ustawie Prawo telekomunikacyjne, zasadnym jest stosowanie wyłączenia dla przedsiębiorców telekomunikacyjnych również w tych przypadkach, w których wymogi dotyczące bezpieczeństwa oraz zgłaszania incydentów w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa dotyczą świadczenia przez przedsiębiorcę telekomunikacyjnego usługi autorytatywnego serwera DNS czy prowadzenia punktu wymiany ruchu internetowego (IXP).

W związku z powyższym proponujemy zmianę definicji punktu wymiany ruchu internetowego w następujący sposób:

*„Podmiot prowadzący punkt wymiany ruchu internetowego (IXP), stanowiący **obiekt element sieciowy współdzielony**, ~~który umożliwia połączenie międzysystemowe pomiędzy więcej niż dwoma niezależnymi systemami autonomicznymi, głównie do celów ułatwienia wymiany ruchu internetowego.~~”*

Niezależnie od powyższego w uzasadnieniu do projektu ustawy albo co najmniej w uzasadnieniu do projektu rozporządzenia w sprawie usług kluczowych należy dopisać fragment wskazujący wprost, iż wyłączenie stosowania przepisów ustawy wobec przedsiębiorców telekomunikacyjnych, przewidziane w art. 1 ust. 2 pkt 1 ustawy o krajowym systemie cyberbezpieczeństwa, dotyczy również przypadków, w których wymogi dotyczące bezpieczeństwa oraz zgłaszania incydentów w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa dotyczą świadczenia przez przedsiębiorcę telekomunikacyjnego usługi autorytatywnego serwera DNS czy prowadzenia punktu wymiany ruchu internetowego (IXP).

z powtórzeniem

Prezes Zarządu

Stefan Kamiński

