KRAJOWA IZBA KOMUNIKACJI ETHERNETOWEJ

ul. Lindleya 16, 02-013 Warszawa
tel. + 48 22 2928700, fax +48 22 2928701
www.kike.pl, e-mail: biuro@kike.pl, grap@kike.pl
KRS 0000316678, REGON 141637224, NIP 9512270210

Warszawa, 4 lutego 2021 r.

ID KIKE: GRAP-55/21

Komitet Rady Ministrów do Spraw Cyfryzacji

ul. Królewska 27
00-060 Warszawa
@: krmc@mc.gov.pl

Kancelaria Prezesa Rady Ministrów
Departament Cyberbezpieczeństwa

ul. Królewska 27
00-060 Warszawa
@: sekretariat.dc@mc.gov.pl

Dotyczy: *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo telekomunikacyjne z dnia 20 stycznia 2021 r.*

Szanowni Państwo,

w imieniu Krajowej Izby Komunikacji Ethernetowej (dalej **KIKE** lub **Izba**), niniejszym przesyłamy uwagi do nowej treści projektu *ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo telekomunikacyjne* (projekt z dnia 20 stycznia 2021 r. – dalej również jako **Projekt**). W niniejszym stanowisku KIKE przedstawia swoje uwagi do Projektu, zestawiając je z treścią ustawy nowelizującej w wersji udostępnionej uprzednio do konsultacji publicznych (tj. z treścią projektu *ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych* z dnia 7 września 2020 r., zwanej dalej **Poprzednim Projektem**).

Zasadnicze zastrzeżenia Izby wzbudza fakt, że aktualna wersja ustawy nowelizującej – wbrew twierdzeniom zawartym w uzasadnieniu ustawy i pojawiającym się w niektórych mediach – nie uwzględnia kluczowych uwag i zastrzeżeń zgłoszonych do Poprzedniego Projektu, a które odnosiły się do naruszenia interesów małych i średnich operatorów telekomunikacyjnych, jakich reprezentuje Izba. Wprowadzone zmiany tylko pozornie eliminują zgłoszone uchybienia i ryzyka, a proces konsultacji stał się przysłowiową zabawą „w kotka i myszkę". Propozycje negowane przez środowisko polskich przedsiębiorców modyfikuje się tak, że na pierwszy rzut oka są one uwzględniane, podczas gdy uważna lektura Projektu prowadzi do wniosków odmiennych[1]. Co więcej, część rozwiązań dla polskich ISP jest daleko bardziej dotkliwych, niż te zawarte w Poprzednim Projekcie. Prowadzi to do wniosku, że autorzy Projektu ani nie uwzględnili specyfiki działalności, jaką prowadzą przedsiębiorcy telekomunikacyjni, ani też dyrektywy płynącej z treści art. 66 *ustawy Prawo przedsiębiorców,*

[1] Przykładowo: wydłuża się po konsultacjach do 7 lat okres na wycofanie sprzętu dostawcy uznanego za dostawcę wysokiego ryzyka, zastrzegając okres pięcioletni na wycofanie sprzętu krytycznego, w sytuacji gdy za sprzęt taki (wymieniony w załączniku nr 3) uznano niemal każdy element warstwy fizycznej sieci telekomunikacyjnej.

nakazującej dokonać oceny projektowanego aktu m.in. pod kątem *przewidywanych skutków społeczno-gospodarczych, w tym oceny wpływu na mikroprzedsiębiorców, małych i średnich przedsiębiorców (…).* A wpływ ten, przy dalszym, bezrefleksyjnym przyjmowaniu kolejnych poprawek, nieuwzgledniających zgłaszanych zastrzeżeń, będzie w ostatecznym rozrachunku dla ISP negatywny, dla niektórych wręcz dramatyczny.

Stanowisko Izby do Projektu składa się z trzech części. **Pierwsza (I)**, to część obejmująca powyższy wstęp i podsumowanie najważniejszych zastrzeżeń, **druga (II)** i zarazem najbardziej obszerna, obejmuje uwagi szczegółowe, oraz **trzecia (III)**, to przesłany już w poprzednich konsultacjach raport przygotowany przez Izbę (oparty na badaniach ankietowych wśród operatorów), który identyfikował zagadnienie wykorzystania przez ISP sprzętu spoza UE, a jednocześnie pokazujący (vide art. 66 *ustawy Prawa przedsiębiorców*) ekonomiczną wagę wadliwie wdrożonych rozwiązań.

I. Zasadnicze zastrzeżenia

1. Polecenia zabezpieczające

1.1. Przyjęte w Poprzednim Projekcie polecenie zabezpieczające obecnie zastosowanie ma znaleźć także wobec przedsiębiorców telekomunikacyjnych (art. 67b *ustawy o krajowym systemie cyberbezpieczeństwa* według Projektu). Co więcej, może ono zostać wydane wobec wszystkich przedsiębiorców telekomunikacyjnych (w tym mikro, małych i średnich ISP), a nie tylko tych, którzy zobowiązani są do posiadania *aktualnych i uzgodnionych planów działań w sytuacjach szczególnych zagrożeń* (czyli z założenia największych przedsiębiorców, których roczne przychody przekraczają 10 mln zł).

1.2. Takim poleceniem zabezpieczającym może być np. nakaz zaprzestania - praktycznie z dnia na dzień - korzystania z określonego sprzętu lub oprogramowania.

1.3. Sygnalizowany wcześniej problem poniesienia przez ISP wysokich kosztów w razie obowiązku wymiany sprzętu takiego czy innego producenta, nie został zatem rozwiązany. Co więcej, rygoryzm ten jest jeszcze daleko bardziej idący. Polecenie – mające mieć rygor natychmiastowej wykonalności – może zobowiązywać ISP do natychmiastowego zaprzestania korzystania z określonego sprzętu.

1.4. Względem Poprzedniego Projektu, teoretycznie (szerzej poniżej) wydłużono pięcioletni termin na wycofanie sprzętu do lat siedmiu, zaś w praktyce w jego miejsce wprowadzono „furtkę" do uczynienia tego natychmiast.

1.5. Dodanie ISP do katalogu podmiotów, wobec których może być wydane polecenie zabezpieczające, nie było wcześniej konsultowane!

2. Złudny termin na usunięcie sprzętu dostawcy wysokiego ryzyka

2.1. Projekt zdaje się wychodzić naprzeciw oczekiwaniom rynku, wydłużając z pięciu, do siedmiu lat, czas na wymianę sprzętu dostawcy uznanego za dostawce wysokiego ryzyka. Faktycznie jest to jednak fikcja.

2.2. Pięcioletni okres został utrzymany dla sprzętu wysokiego ryzyka, wymienionego w załączniku nr 3 do Projektu. Uważna lektura tego dokumentu prowadzi do wniosku, że za taki sprzęt (podlegający usunięciu w ciągu 5 lat) uznano niemal każdy element warstwy fizycznej sieci telekomunikacyjnej. To kolejny argument pokazujący fasadowość poprzednich konsultacji.

2.3. Konstrukcja nakazania wycofania sprzętu określonego dostawcy czy zakazania stosowania takiego sprzętu, faktycznie wpłynie negatywnie na poziom bezpieczeństwa w sieciach. Używane będą urządzenia/sprzęty „niemarkowe", które staną się atrakcyjne z uwagi na niższą cenę, a faktycznie korzystanie z nich – jako urządzeń „no name" - doprowadzi do tego, że producentom przestanie się opłacać dbać o markę i poziom zabezpieczeń (np. aktualizację oprogramowania).

3. Cyberbezpieczeństwo a współpraca hurtowa

3.1. Błędne i nieprawdziwe jest założenie, że nałożenie obowiązku wymiany sprzętu (oprogramowania) przez jedynie największych przedsiębiorców telekomunikacyjnych przyczyni się do zwiększenia poziomu (cyber)bezpieczeństwa.

3.2. Projekt przewiduje, że wymiana sprzętu w ciągu 7 (czy 5) lat dotyczy tylko ISP posiadających *aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, o których mowa w art. 176a prawa telekomunikacyjnego*.

3.3. Projektodawcy zdają się nie rozróżniać warstwy fizycznej od warstwy logicznej sieci, jako zespołu „połączonych ze sobą naczyń", niekoniecznie należących do jednego i tego samego operatora.

3.4. W powyższym kontekście Projekt kompletnie pomija kwestie związane ze współkorzystaniem z sieci telekomunikacyjnych przez różnych operatorów, co na rynku określane jest jako współpraca hurtowa. Ten rodzaj współdzielenia sieci i usług promowany jest nie tylko przez polskiego regulatora (Prezesa UKE), ale także przez ustawodawcę unijnego[2].

3.5. Projekt oparto na błędnym założeniu, że z sieci telekomunikacyjnych dużych operatorów korzystają wyłącznie inni, duzi operatorzy. Nie jest to prawdą, a nakazanie usunięcia sprzętu tylko takim przedsiębiorcom, nie wpłynie na poprawę bezpieczeństwa w sytuacji, gdy omawiani przedsiębiorcy w ramach współpracy hurtowej korzystają z sieci mniejszych ISP (i vice versa).

3.6. W praktyce, kwestie związane z dostępem hurtowym mogą mieć szeroki wpływ na rzeczywiste skutki proponowanej regulacji, albowiem możliwe jest wystąpienie co najmniej czterech scenariuszy, opisanych szczegółowo w cz. II stanowiska KIKE. Jednym z możliwych scenariuszy jest sytuacja, w której duzi operatorzy, objęci nakazem uregulowanym w Projekcie, będą zmuszeni wycofać z użytkowania określone typy produktów, a zmiana ta nie będzie wymagać żadnych zmian konfiguracji w sieci operatorów korzystających (w tym nie będzie wymagać zmiany urządzeń używanych przez operatorów korzystających). Uproszczając – do sieci dostępowej (objętej nakazem wycofania urządzeń) - będzie podłączone urządzenie, którego dostawca został uznany za dostawcę wysokiego ryzyka.

4. Wadliwy sposób przeprowadzenia konsultacji co do części Projektu

4.1. Konsultacje pokierowano wadliwie, utrudniając prowadzenie rzetelnego dialogu strony społecznej (w tym m.in. zrzeszającej małych i średnich operatorów KIKE) z projektodawcami.

[2] Wystarczy sięgnąć do przepisów wdrażanego obecnie EKŁE i przygotowanego na jego bazie projektu PKE, czy też tzw. rozporządzenia GBER lub tzw. dyrektywy kosztowej.

4.2. Poprzedni Projekt przewidywał zmiany w *ustawie o krajowym systemie cyberbezpieczeństwa* i w *ustawie – prawo zamówień publicznych*. Obecnie jest to projekt zmieniający *ustawę o krajowym systemie cyberbezpieczeństwa* i *ustawę – prawo telekomunikacyjne.*

4.3. Zawarte wyżej uwagi pokazują, że konsultacjom nie został poddany szereg nowych rozwiązań, w tym objęcie ISP poleceniami zabezpieczającymi, czy koncepcja operatora sieci komunikacji strategicznej.

5. Brak uwzględnienia skutków ekonomicznych Projektu

5.1. KIKE ponownie podnosi, że Projekt nie uwzględnia skutków ekonomicznych. Przez wprowadzenie instytucji polecenia zabezpieczającego, nie został rozwiązany problem konieczności poniesienia ogromnych kosztów wymiany sprzętu, sygnalizowany przez KIKE jeszcze na etapie konsultacji społecznych.

5.2. KIKE raz jeszcze załącza wykonany w październiku 2020 roku *Raport dotyczący skali wykorzystania w sektorze telekomunikacyjnym sprzętu dostawców pochodzących spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego,* z którego jednoznacznie wynika, jaki będzie średni koszt wymiany sprzętu wśród małych i średnich ISP.

5.3. Ewentualne wystosowanie *polecenia zabezpieczającego* w stosunku do ISP, który swoją infrastrukturę zbudował wyłącznie w oparciu o sprzęt jednego dostawcy (z badania wynika, że 51% ankietowanych podjęło taką decyzję), spowoduje konieczność natychmiastowego zaprzestania prowadzenia przez tego ISP działalności gospodarczej. Obrazowo rzecz ujmując, nie będzie miał on sprzętu, z którego będzie mógł korzystać, świadcząc usługi.

6. Brak zagwarantowania konstytucyjnych praw do obrony w sądzie

6.1. Przewidziane w projekcie środki ochrony prawnej są iluzoryczne, pokazują, iż podejmowane decyzje mają mieć charakter polityczny, a nie rzeczowy, służący zapewnieniu cyberbezpieczeństwa.

6.2. Prawdo do złożenia skargi do WSA jest fikcją w sytuacji, gdy, ani sąd, ani strona nie poznają faktycznego uzasadnienia wydanej decyzji.

6.3. Koncepcja, iż indywidualna decyzja administracyjna, wydana wobec konkretnego dostawcy sprzętu, ma wywoływać skutki prawne wobec nie objętych jej treścią operatorów, jest bezpodstawna i nie ma oparcia w przepisach prawa krajowego i unijnego.

***

KIKE wyraża nadzieję, że wskazane powyżej zastrzeżenia i uwagi zostaną nie tylko przez autorów Projektu przemyślane, ale również uwzględnione w ostatecznej wersji Projektu. Jego ponowne przygotowanie – mając na względzie ważkość materii regulowanej w Projekcie – powinno skutkować przeprowadzeniem kolejnej rundy konsultacji społecznych.

W załączeniu: **cz. II - uwagi szczególne** oraz **raport KIKE** z 5.10.2020 roku.

Z poważaniem,

Karol Skupień
Prezes KIKE/GRAP KIKE

Łukasz Bazański
GRAP KIKE/ itB Legal