04.03.2020 r.

**Zestawienie zgłoszonych uwag do projektu rozporządzenia Ministra Cyfryzacji w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług – konsultacje**

**UZUPEŁNIENIE TABELI**

Uwagi zgłoszone przez:

* Polska Izba Komunikacji Elektronicznej (zgłoszono 17.02.2020 - po terminie)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr uwagi** | **Jednostka redakcyjna projektu** | **Zgłaszający** | **Treść uwagi** | **Stanowisko MC** |
|  | Ogólna | PIKE | Projekt rozporządzenia reguluje istotną z punktu widzenia rynku telekomunikacyjnego kwestię, jaką jest zapewnienie bezpieczeństwa  i integralności sieci oraz usług telekomunikacyjnych. Należy jednak wskazać, że jego treść wymaga znaczących zmian. Konieczna jest bowiem szersza debata na temat wymaganych poziomów bezpieczeństwa w sieciach operatorów z uwzględnieniem zakresu świadczonych przez nich usług oraz wielkości ich udziału w rynku.  W tym względzie należy zwrócić uwagę na konieczność dokonania przeglądu proponowanych działań pod kątem ich skuteczności oraz ich proporcjonalności przy zapewnianiu bezpieczeństwa i integralności sieci oraz usług. Należy przede wszystkim uwzględnić fakt, że projekt rozporządzenia powinien obejmować minimalny zakres środków jakie mają zastosować przedsiębiorcy telekomunikacyjni. Tymczasem, zdaniem Izby katalog działań przedstawiony w projekcie rozporządzenia jest nazbyt szeroki i obejmuje większość działań wskazanych w wytycznych ENISA z 2014 r.  Ponadto, należy również uzupełnić uzasadnienie do projektu rozporządzenia o analizy dotyczące tego, jakie środki techniczne  i organizacyjne uznano za nadmiarowe i nie zamieszczono ich  w projekcie rozporządzenia. | Wyjaśnienie.  Ocena istniejących zagrożeń, dokumentowanie środków bezpieczeństwa czy zasad dostępu to absolutne podstawy, które już powinny u większości przedsiębiorców mieć miejsce.  Obowiązek podejmowania proporcjonalnych i uzasadnionych środków mających na celu zapewnienie bezpieczeństwa oraz integralności sieci i usług funkcjonuje od 2004 r. tj, od dnia wejścia w życie ustawy PT. Natomiast projektowane rozporządzenie określa minimalne środki techniczne i organizacyjne oraz metody zapobiegania zagrożeniom, wprowadzając i precyzując jednolite wymogi dla wszystkich przedsiębiorców telekomunikacyjnych.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | Ogólna | PIKE | PIKE uprzejmie dziękuje za możliwość udziału w procesie legislacyjnym i wyraża nadzieję, że opisane w niniejszym piśmie uwagi i propozycje zostaną przez Ministra Cyfryzacji uwzględnione w toku dalszych prac. Izba pragnie zwrócić uwagę przede wszystkim na wskazaną w art. 13a dyrektywy 2009/140/WE zasadę proporcjonalności środków  w stosunku do istniejącego ryzyka. Z tego względu minimalny zestaw środków określony w projekcie rozporządzenia powinien być jak najmniejszy, aby pozwolić przedsiębiorcom na elastyczne reagowanie na zagrożenia. | Wyjaśnienie.  Użyte w rozporządzeniu środki i metody są dalej zgodne z postanowieniami art. 175 i następnymi. Wskazane środki i metody nadal pozwalają na swobodny dobór szczegółowych sposobów realizacji obowiązku ustawowego.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | § 2 pkt 1 | PIKE | **Obowiązek z § 2 pkt 1 projektu rozporządzenia powinien zostać usunięty**, gdyż nie wnosi on żadnej nowej treści, a jedynie powtarza obowiązki przygotowania dokumentacji wskazanych w pkt 2-14. Dodatkowo zapis ten nie bierze pod uwagę faktu, że część działań z pkt 2-14 nie dotyczy przygotowania dokumentacji w zakresie procedur czy zasad, ale podejmowania określonych działań wynikających z tych procedur i zasad. Nie jest więc możliwe aktualizowanie takich dokumentów. Jednocześnie, Izba podkreśla swoje zastrzeżenia co do konieczności automatycznej aktualizacji większości z tych dokumentów. | Wyjaśnienie.  Obowiązek posiadania dokumentacji wiąże się z zapewnieniem śladu audytowego tj. udowodnienia, że dany środek bezpieczeństwa jest proporcjonalny do oszacowanego ryzyka.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | § 2 pkt 2 | PIKE | Należy wskazać na szeroki zakres obowiązku przedstawiania wykazu infrastruktury telekomunikacyjnej i oprogramowania oraz na jego nieproporcjonalność. Zdaniem izby **obowiązek z § 2 pkt 2 projektu rozporządzenia powinien być ograniczony tylko do infrastruktury  i oprogramowania krytycznego**, a nie wszelkich elementów sieci telekomunikacyjnej. | Uwaga nieuwzględniona.  Chodzi tu o wykaz obejmujący całość infrastruktury telekomunikacyjnej i oprogramowania służących do świadczenia usług telekomunikacyjnych.  Prowadzenie pełnego wykazu infrastruktury umożliwi przedsiębiorcom dokonanie właściwego szacowania ryzyka. Bez przeprowadzenia pełnej inwentaryzacji infrastruktury nie jest możliwe określenie jej własności i odpowiedzialności w organizacji, stopnia jej istotności dla działalności czy też zasad korzystania z niej. W opinii MC nie jest możliwe przeprowadzenie szacowania ryzyka z pominięciem tego kroku.  Na konferencji:  Zmieniono brzmienie przepisu § 2 pkt 2. Ograniczono do istotnej infrastruktury. |
|  | § 2 pkt 3 | PIKE | Przedmiotowy obowiązek jest wyjątkowo trudny do realizacji dla przedsiębiorców telekomunikacyjnych. Analiza dokumentacji ENISA  (w języku angielskim) wymaga bardzo specjalistycznej wiedzy oraz dodatkowego personelu. Ponadto zagrożenia wymienione przez ENISA nie muszą być głównymi zagrożeniami występującymi  w Polsce. Zdaniem Izby, **obowiązek określony w § 2 pkt 3 projektu rozporządzenia powinien zostać całkowicie przeformułowany**. Po pierwsze, materiałem źródłowym do identyfikacji zagrożeń przez przedsiębiorców powinny być analizy UKE lub NASK dotyczące incydentów w Polsce oraz inne raporty oparte na analizach opracowanych przez ENISA. Po drugie, obowiązek ten powinien raczej ograniczać się do zapoznania z tymi raportami, a nie dotyczyć tworzenia nowej dokumentacji na ten temat od podstaw (taki obowiązek powstaje niejako przy okazji połączenia tego obowiązku z projektowanym obowiązkiem z pkt 1 dotyczącym opracowania odpowiedniej dokumentacji).  Co więcej, obowiązek z pkt 3(podobnie jak i cały projekt rozporządzenia) powinien dotyczyć jedynie zagrożeń, które miały istotny wpływ na funkcjonowanie sieci lub usług. Tymczasem, dotyczy on wszystkich incydentów, nawet tych błahych. Izba zwraca również uwagę na fakt błędnego odesłania w tym punkcie do art. 9 lit. b i e rozporządzenia w sprawie ENISA. Mianowicie, rozporządzenie w sprawie ENISA nie definiuje samodzielnie pojęcia „incydent”, tylko odwołuje się w tym zakresie do art. 4 pkt 7 dyrektywy (UE) 2016/1148 w sprawie środków na rzecz wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych na ternie Unii, której przepisy z kolei nie stosują się do przedsiębiorców telekomunikacyjnych niebędących dostawcami usług kluczowych. Tym samym określenie „incydent” jest definiowane stosownie do działalności operatorów usług kluczowych, która nie zawsze będzie odpowiadać działalności wszystkich przedsiębiorców telekomunikacyjnych. | W ocenie MC dokument jest wyczerpujący i nie ma potrzeby powoływać się na inne publikacje. Należy dodatkowo wskazać, że zgodnie z upoważnieniem ustawowym należy opierać się przede wszystkim na publikacjach ENISA.  Termin „incydent” pojawia się tylko w kontekście dokumentu ENISA. Należy wskazać, że w nowym EKŁE zamiast „naruszeń” są już „incydenty”.  Na konferencji:  Zmieniono brzmienie przez usunięcie odesłania do dokumentów ENISA. Dodatkowo, zostanie rozszerzone uzasadnienie. |
|  | § 2 pkt 4 | PIKE | Obowiązek z pkt 4 § 2 projektu rozporządzenia jest właściwie kontynuacją obowiązku z pkt 3 i nie powinien być od niego oddzielony. Wraz z pkt 1 oznacza on obowiązek przygotowania dokumentacji (i jej aktualizacji) w zakresie prawdopodobieństwa wystąpienia wszelkich naruszeń w sieci danego operatora. Zdaniem Izby **obowiązek ten jest nieadekwatny do celu jakim jest zwalczanie istotnych zagrożeń  w sieciach telekomunikacyjnych** (dotyczy wszelkich naruszeń). Ponadto należy przeanalizować, czy środek ten powinien znaleźć się  w katalogu minimalnych środków jakie muszą podjąć wszyscy przedsiębiorcy telekomunikacyjni. | Uwaga nieuwzględniona.  MC nie stoi na stanowisku, aby udokumentowana ocena zagrożeń była nieadekwatnym środkiem realizacji celu ochrony sieci.  Na konferencji:  PIKE przyjęło wyjaśnienia. |
|  | § 2 pkt 5 | PIKE | Działalnie z § 2 pkt 5 projektu rozporządzenia jest związane bezpośrednio z pkt 3 i 4 i dlatego powinien być opracowany łącznie  z nimi. Tym samym **regulacji tej dotyczą te same zarzuty, które Izba podniosła w pkt 3 i 4 stanowiska.** | Wyjaśnienie.  Punkty 3-6 stanowią całość, jednak dla czytelności zostały rozbite.  Na konferencji:  Przyjęto nowe brzmienie przepisu. |
|  | § 2 pkt 6 | PIKE | Ponownie, **działanie z § 2 pkt 6 projektu rozporządzenia należy rozpatrywać łącznie z działaniami z pkt 3, 4 i 5**. Stosują się zatem do niego podniesione już wcześniej zarzuty Izby, przede wszystkim dotyczące obowiązku podejmowania określonych działań (i dokumentowania tego faktu) w stosunku do każdego rodzaju incydentu/zagrożenia, a nie jak stanowi art. 175a tylko tych, które miały istotny wpływ na funkcjonowanie sieci lub usług. | Wyjaśnienie.  Punkty 3-6 stanowią całość, jednak dla czytelności zostały rozbite.  Na konferencji:  Przyjęto nowe brzmienie przepisu. |
|  | § 2 pkt 7 | PIKE | § 2 pkt 7 projektu rozporządzenia jest pierwszym i jedynym, który skupia się na kluczowych/istotnych elementach sieci telekomunikacyjnych, które powinny być chronione. Izba nie ma zastrzeżeń co do konieczności przygotowania takich procedur, ale wskazuje, że sam obowiązek może okazać się niewystarczający dla spójnego zwalczania zagrożeń. **Działanie to powinno zostać uzupełnione o niewiążące rekomendacje UKE i NASK w zakresie realizacji tego obowiązku**. Brak takich rekomendacji oznacza brak spójności działań operatorów w ochronie swoich sieci, co także utrudni UKE i NASK analizę zwalczania zagrożeń.  **Konieczne jest uściślenie, że nie chodzi w tym działaniu  o przetwarzanie danych tranzytowanych w sieciach telekomunikacyjnych w ramach usługi dostępu do sieci Internet,  a jedynie o dane wrażliwe znajdujące się w systemach przedsiębiorców telekomunikacyjnych**. | Wyjaśnienie.  Rozporządzenie realizuje delegację ustawową, która umożliwia odniesienie się do dokumentów KE i ENISA, co też uczyniono.  Nic nie stoi na przeszkodzie, aby stosować też inne dobre praktyki czy rekomendacje.  W zakresie danych tranzytowych uwaga jest nieuwzględniona. Niedopuszczalne jest pomijanie zabezpieczeń dla danych tranzytowych.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | § 2 pkt 8 | PIKE | § 2 pkt 8 projektu rozporządzenia częściowo zawiera się już  w działaniach z pkt 7. Ustanowienie zasad i procedur dostępu do kluczowych zasobów oznacza również wdrożenie tych procedur. Jednocześnie pojawia się tu nowy obowiązek jakim jest stałe **monitorowanie tego dostępu**, przy czym **projekt rozporządzenia nie wyjaśnia na czym takie działanie miałoby polegać**.  Odrębnego omówienia wymaga kwestia środków reagowania  na nieuprawniony dostęp lub próbę takiego dostępu. Z uwagi na to,  że mówimy tu o włamaniach do systemów informatycznych operatora należy uznać to zagrożenie za mające znaczący wpływ na integralność sieci oraz usług. W tym wypadku należy wskazać, że działania samych operatorów mogą okazać się niewystarczające i potrzebne będzie rządowe wsparcie przy zwalczaniu takich włamań. Nie może być tak,  że operator sam musi się uporać z atakami hackerskimi i to tylko poprzez zwiększanie nakładów na swoje zabezpieczenia. W tym względzie ewentualne działania przedsiębiorcy muszą być skorelowane z aktywnymi działaniami policji oraz NASK. **Jedyne konkretne działania, jakie operator może sam podjąć zostały opisane w art. 175c ust. 1 Pt, przy czym środki te nie zostały wymienione w projekcie rozporządzenia**. | Wyjaśnienie.  Prośba o propozycje na konferencji uzgodnieniowej.  Propozycja podłączenia operatorów do KSC w 2017 r. nie spotkała się z aprobatą rynku.  Na konferencji:  MC stoi na stanowisku, że czym innym jest ustanowienie zasad dostępu, a czym inne wprowadzenie zabezpieczeń przed nieuprawnionym dostępem.  PIKE przyjęło wyjaśnienia. |
|  | § 2 pkt 9 | PIKE | Kwestią procedur dostępu do przetwarzanych danych zajmują się już pkt 7 i 8 § 2 projektu rozporządzenia. Zdaniem Izby nie jest potrzebne wyodrębnianie zasad bezpieczeństwa ich przetwarzania, jak to czyni pkt 9 § 2 projektu, od zasad ochrony danych na dostęp do nich opisanych w pkt 7 i 8. **Obie te materie są ze sobą powiązane i powinny być uregulowane razem.** | Wyjaśnienie.  W opinii projektodawcy kwestie ustanawiania procedur i wdrażanie zabezpieczeń to odrębne działania.  Są one uregulowane w jednym rozporządzeniu i są czytane razem; rozbito je dla czytelności.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | § 2 pkt 10 | PIKE | Zdaniem PIKE pkt 10 § 2 projektu rozporządzenia jest już zrealizowany przy okazji działań z pkt 7-9. Podobnie jak w przypadku innych działań, przedsiębiorca telekomunikacyjny, zwłaszcza mały lub średni nie może zostać pozostawiony samemu sobie przy zwalczaniu przestępstw hackerskich. Jego działania powinny być skorelowane z działaniami odpowiednich organów ścigania. Zdaniem Izby pasywne działanie samych przedsiębiorców telekomunikacyjnych polegające  na zwiększaniu bezpieczeństwa swoich sieci nie wyeliminuje skutecznie zjawisk hackerskich. Do tego **potrzebne są aktywne działania organów ścigania**.  Dodatkowo jak wskazano w pkt 7 stanowiska, w pkt 10 § 2 projektu także powinno być **uściślone, że nie chodzi przy tym działaniu o dane transmitowane w sieciach telekomunikacyjnych w ramach usługi zapewnienia dostępu do sieci Internet**. | Wyjaśnienie.  Niniejsze rozporządzenie nie reguluje działań Policji.  W zakresie danych tranzytowych uwaga jest nieuwzględniona. Niedopuszczalne jest pomijanie zabezpieczeń dla danych tranzytowych.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | § 2 pkt 11 | PIKE | Prawodawca w § 2 pkt 11 projektu rozporządzenia nakazuje analizę wszystkich umów międzyoperatorskich pod kątem bezpieczeństwa  i integracji sieci oraz usług. Obecnie co do zasady jest to już wykonywane, ale przede wszystkim w kontekście interoperacyjności usług telekomunikacyjnych (telefonicznych oraz wymiany danych w sieciach). **Przedmiotowy obowiązek można natomiast rozumieć jako konieczność analizy wszystkich umów międzyoperatorskich pod katem zwalczania cyberprzestępstw czy zapobiegania fizycznym uszkodzeniom sieci telekomunikacyjnych. Taki nowy obowiązek wymagałby przerabiania większości umów międzyoperatorskich  w sposób wymuszający ingerencję w transmisję danych**. | Wyjaśnienie.  Środek z pkt 11 wskazuje na obowiązek identyfikacji zagrożeń, a nie przerabiania większości umów międzyoperatorskich  w sposób wymuszający ingerencję w transmisję danych.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | § 2 pkt 12 | PIKE | Obowiązek z § 2 pkt 12 projektu rozporządzenia znacząco wykracza poza delegację ustawową i jest nieproporcjonalny do celu, jakim jest zwalczanie zagrożeń. Projekt bowiem nakazuje ciągłe monitorowanie stanu sieci i jego dokumentowanie. Taka jego konstrukcja może być rozumiana jako konieczność ciągłego monitorowania wszelkich elementów sieci (nawet tych nieistotnych) i sporządzania z tego niepotrzebnej dokumentacji. Tymczasem **obowiązek ten powinien się skupić wyłącznie na monitorowaniu i dokumentowaniu naruszeń bezpieczeństwa i integralności, mających istotny wpływ  na funkcjonowanie sieci lub usług**.  Wyjaśnienia wymaga również kwestia ustalenia przyczyn naruszenia bezpieczeństwa. W opinii Izby operator powinien jedynie określać rodzaj naruszenia, natomiast wszelkie bardziej szczegółowe dane powinien przekazywać wyłącznie w wypadku posiadania ich przy okazji świadczenia usług. Przepis ten nie może nakazywać przedsiębiorcom telekomunikacyjnym prowadzenie samodzielnego dochodzenia w celu wykrycia szczegółowych źródeł naruszenia bezpieczeństwa sieci, zwłaszcza tych pochodzących spoza jego sieci. | Wyjaśnienie.  W opinii MC, nie jest możliwe monitorowanie wyłącznie naruszeń bezpieczeństwa i integralności mających istotny wpływ na funkcjonowanie sieci lub usług. Z definicji, wymaga to monitoringu sieci pod kątem różnych zagrożeń. Nie oznacza to obowiązku logowania wszystkiego czy pełnej retencji.  Na konferencji:  Przedstawiono wyjaśnienie MC. |
|  | § 2 pkt 13 | PIKE | Izba wskazuje, że **§ 2 pkt 13 projektu rozporządzenia powinien uwzględniać procedurę zgłoszeń naruszeń z art. 175a ust. 1b oraz ust. 2 Pt.** | Uwaga uwzględniona.  § 13 zostanie zmieniony.  Na konferencji:  Przepis będzie się odnosił do „wewnętrznych procedur”. |
|  | § 2 pkt 14 | PIKE | Zdaniem Izby obowiązek z § 2 pkt 14 projekturozporządzenia stanowi najtrudniejszy do realizacji obowiązek, zwłaszcza z uwagi na brak jego dookreślenia i liczne przesłanki jego wykonania. W opinii Izby taka **ocena bezpieczeństwa sieci powinna być dokonywana nie częściej niż raz do roku**. Dodatkowo, zamiast przeprowadzać ją automatycznie  po określonym czasie, **powinna ona następować po wystąpieniu poważnych naruszeń mających istotny wpływ na funkcjonowanie sieci i usług**.  Istotnym problemem jest konieczność wykonania takiej oceny po każdy naruszeniu integralności sieci o istotnym wpływie na sieć lub usługi.  **W przypadku samych prób hackerskich traktowanych jako naruszenie bezpieczeństwa, zdaniem Izby nie jest konieczna obligatoryjna ocena bezpieczeństwa sieci.** Może to oznaczać w przypadku częstych ataków hackerskich konieczność oceniania bezpieczeństwa sieci co miesiąc. Ponadto, Izba uważa, że brak jest potrzeby przeprowadzania takiej oceny w sytuacji, gdy powzięto środki przeciwdziałające takim naruszeniom.  Jeszcze mniej jasna jest przesłanka dokonywania oceny w przypadku stwierdzenia podatności sieci na zagrożenie zwiększające poziom ryzyka wystąpienia naruszenia o istotnym wpływie na sieć. Tak obowiązek można rozumieć jako konieczność permanentnego oceniania bezpieczeństwa swojej sieci, a przy okazji nieprzerwanego monitorowania możliwych zagrożeń. Operatorzy będą musieli ponosić duże wydatki związane z tą ciągłą oceną, co jest działaniem nie tylko nieproporcjonalnym, ale przede wszystkim niecelowym. W opinii Izby, **taka aktualizacja oceny nie może być oceniana jako minimalny środek mający na celu zapewnienie bezpieczeństwa**. | Wyjaśnienie.  Zgodnie z projektem, ocena bezpieczeństwa musi nastąpić:   1. raz na rok lub 2. po każdym naruszeniu bezpieczeństwa lub integralności sieci lub 3. po każdym wykryciu podatności.   Okresowe, coroczne sprawdzanie systemów wydaje się standardową, zalecaną praktyką.  Nie musi to koniecznie być pełen audyt; nie jest też sugerowane, aby była to ocena zlecana na zewnątrz – może to zostać dokonane własnymi środkami przedsiębiorcy.  Po konferencji:  MC przygotowało nowe brzmienie przepisu. |