Stanisław Piątek*

Obowiązki przedsiębiorców telekomunikacyjnych w zakresie cyberbezpieczeństwa

Spis treści

Streszczenie

W artykule przedstawiono status przedsiębiorców telekomunikacyjnych w sprawach dotyczących cyberbezpieczeństwa z uwzględnieniem przepisów Unii Europejskiej i przepisów krajowych. Mimo wyłączenia przedsiębiorców telekomunikacyjnych z zakresu stosowania ogólnych przepisów o cyberbezpieczeństwie, podmioty te są w ramach regulacji sektorowej zobowiązane do realizacji obowiązków zabezpieczającymi sieci, usługi i komunikaty przed zagrożeniami, eliminowania tych zagrożeń oraz informowania użytkowników usług i organów państwowych o występujących zagrożeniach. Prezes UKE zapewnia przepływ informacji o incydentach w sektorze telekomunikacyjnym do właściwych organów w krajowym systemie cyberbezpieczeństwa.

Słowa kluczowe: cyberbezpieczeństwo; przedsiębiorca telekomunikacyjny; łączność elektroniczna; użytkownicy końcowi; incydent; obowiązki informacyjne.

JEL: K23, K24

I. Wprowadzenie

Przedsiębiorcy telekomunikacyjni zostali wyłączeni z zakresu zastosowania ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[1] (dalej: uksc) w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów, a jednocześnie nie ulega wątpliwości, że ich działalność ma istotny wpływ na stan bezpieczeństwa cybernetycznego. Celem artykułu jest analiza

* Profesor Wydziału Zarządzania UW, Katedra Prawnych Problemów Administracji i Zarządzania; e-mail: spiatek@wz.uw.edu.pl; https://orcid.org/0000-0003-1892-9283.

[1] DzU 2018, poz. 1560 ze zm.

i ocena sposobu, w jaki przedsiębiorcy telekomunikacyjni zostali włączeni w system ochrony przed zagrożeniami w zakresie cyberbezpieczeństwa, mimo wyłączenia przewidzianego w art. 1 ust. 2 pkt 1 uksc. Usytuowanie przedsiębiorców telekomunikacyjnych w systemie cyberbezpieczeństwa wynika z przepisów krajowych, ale podstawowe rozwiązania w tym zakresie są konsekwencją rozwiązań przyjętych w prawie Unii Europejskiej. Odrębności dotyczące przedsiębiorców telekomunikacyjnych dotyczą zarówno obowiązków związanych z przeciwdziałaniem zagrożeniom w zakresie cyberbezpieczeństwa i zwalczania zagrożeń, jak i informowania o wystąpieniu takich zagrożeń. Dzięki powierzeniu odpowiednich zadań Prezesowi Urzędu Komunikacji Elektronicznej (UKE) zapewniono transmisję informacji o incydentach występujących w sektorze telekomunikacyjnym do właściwych ogniw krajowego systemu cyberbezpieczeństwa. Struktura regulacji sektorowej dotyczącej cyberbezpieczeństwa w telekomunikacji odpowiada układowi obowiązków dotyczących operatorów usług kluczowych, przewidzianych w ogólnych przepisach dotyczących cyberbezpieczeństwa (Kitler, Taczkowska-Olszewska i Radoniewicz, 2019, art. 1 NB. 3–14).

II. Unijne podstawy prawne cyberbezpieczeństwa w sektorze łączności elektronicznej

Odrębność prawnych rozwiązań dotyczących cyberbezpieczeństwa w sektorze łączności elektronicznej ma dłuższą historię w prawie unijnym (Rojszczak, 2018, s. 200 i n.). Unijne rozwiązania w zakresie cyberbezpieczeństwa w sektorze łączności elektronicznej zostały ukształtowane przepisami rozdziału IIIa dodanego w roku 2009 w dyrektywie ramowej 2002/21/WE[2]. Artykuł 13a dyrektywy ramowej zobowiązuje do stosowania właściwych środków technicznych i organizacyjnych w razie wystąpienia zagrożenia dla bezpieczeństwa sieci i usług, zapewniających poziom bezpieczeństwa proporcjonalny do istniejącego ryzyka, z uwzględnieniem aktualnego stanu wiedzy i technologii. Przedsiębiorstwa mają chronić integralność sieci w celu zapewnienia ciągłości świadczenia usług. Przedsiębiorstwa powinny zawiadamiać regulatora o każdym naruszeniu bezpieczeństwa lub istotnej utracie integralności sieci. Przewidziano wzajemne informowanie się przez państwa członkowskie w tych sprawach oraz informowanie europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) o występowaniu zagrożeń. Zgodnie z art. 13b dyrektywy ramowej regulator krajowy powinien być uprawniony do wydawania przedsiębiorcom wiążących instrukcji w sprawach bezpieczeństwa sieci i usług, żądania od nich informacji oraz poddania się na własny koszt audytowi bezpieczeństwa.

Dyrektywa NIS[3] potwierdziła odrębność sektora łączności elektronicznej w sprawach cyberbezpieczeństwa. Przepis art. 1 ust. 3 dyrektywy NIS stanowi, że wymogi dotyczące bezpieczeństwa i zgłaszania incydentów przewidziane w dyrektywie nie mają zastosowania do przedsiębiorstw, które podlegają wymogom art. 13a i 13b dyrektywy ramowej 2002/21/WE. W motywie 7 dyrektywy NIS uzasadnia się, iż obowiązki nakładane na operatorów usług kluczowych i dostawców usług cyfrowych nie powinny mieć zastosowania do przedsiębiorstw udostępniających publiczne sieci łączności lub świadczących publicznie dostępne usługi łączności elektronicznej w rozumie-

[2] Dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7.03.2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa) (DzU L 108/33 z 24.04.2002 ze zm.).

[3] Dyrektywa 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 194/1 z 19.07.2016).

niu dyrektywy ramowej, gdyż przedsiębiorcy ci podlegają szczegółowym wymogom w zakresie bezpieczeństwa i integralności ustanowionym w tej dyrektywie.

Powyższy stan powinien być utrzymany również po wdrożeniu Europejskiego kodeksu łączności elektronicznej (EKŁE)[4]. Do grudnia 2020 roku państwa członkowskie powinny implementować postanowienia EKŁE, które zastępują rozwiązania wprowadzone dyrektywą ramową 2002/21/WE i kompleksowo regulują kwestie cyberbezpieczeństwa w sektorze łączności elektronicznej. W art. 2 pkt 42 EKŁE zdefiniowano „incydent związany z bezpieczeństwem" jako zdarzenie, które ma rzeczywisty niekorzystny skutek dla bezpieczeństwa sieci lub usługi łączności elektronicznej. Zdarzenie o rzeczywistym (*actual*) skutku, to zdarzenie które faktycznie się zmaterializowało. Państwa członkowskie powinny nałożyć na dostawców sieci i usług obowiązki dotyczące podejmowania proporcjonalnych środków technicznych i organizacyjnych w przypadku wystąpienia zagrożeń. Środki te powinny zapewnić poziom bezpieczeństwa proporcjonalny do istniejącego ryzyka z uwzględnieniem aktualnego stanu wiedzy i technologii. Motyw 94 EKŁE precyzuje jakie kwestie należy uwzględniać. W odniesieniu do bezpieczeństwa sieci i urządzeń uwzględnia się bezpieczeństwo fizyczne i bezpieczeństwo środowiska, bezpieczeństwo dostaw, kontrolę dostępu do sieci i integralność sieci. W odniesieniu do postępowania w sprawie incydentów związanych z bezpieczeństwem należy uwzględnić procedury postępowania w przypadku incydentów, zdolności wykrywania incydentów, zgłaszania incydentów związanych z bezpieczeństwem i informowanie o nich. W odniesieniu do zarządzania ciągłością działalności uwzględnia się strategię ciągłości usług i plany awaryjne, zdolności w zakresie przywracania gotowości do pracy po katastrofie, w odniesieniu zaś do monitorowania, kontroli i testowania – strategie monitorowania i rejestrowania, ćwiczenia w zakresie planów awaryjnych, testowanie sieci i usług, oceny bezpieczeństwa i monitorowanie zgodności. Należy również zapewnić zgodność projektowanych środków z normami międzynarodowymi. Szczególne podejście zaleca się w odniesieniu do bardzo rozpowszechnionych obecnie usług łączności interpersonalnej niewykorzystujących numerów (np. WhatsApp, Facebook Messenger), na które rozszerzono obowiązywanie EKŁE. Zgodnie z motywem 95 podlegają one również wymogom dotyczącym bezpieczeństwa. Jednak ze względu na to, że dostawcy tych usług zazwyczaj nie sprawują rzeczywistej kontroli nad transmisją sygnałów w sieciach, stopień ryzyka w przypadku takich usług można uznać pod pewnymi względami za niższy niż w przypadku tradycyjnych usług łączności elektronicznej. Dlatego też środki podejmowane przez dostawców tych usług powinny być łagodniejsze.

Krajowe wymagania w zakresie cyberbezpieczeństwa w sektorze łączności elektronicznej nie powinny utrudniać dostępu do poszczególnych rynków krajowych. Dlatego przepis art. 40 ust. 1 EKŁE powierza ENISA działania mające na celu uniknięcie powstawania rozbieżnych krajowych wymogów dotyczących bezpieczeństwa, które mogą tworzyć ryzyko dla bezpieczeństwa i barier dla rynku wewnętrznego.

Przepisy art. 40 EKŁE precyzują obowiązki dostawcy usług związane z występowaniem incydentów bezpieczeństwa, w szczególności obowiązki związane z powiadamianiem właściwych organów, użytkowników usług i sieci oraz podawaniem informacji o najpoważniejszych incydentach do wiadomości publicznej. Kluczowym elementem reakcji dostawców sieci i usług na incydenty związane z bezpieczeństwem jest powiadamianie właściwych organów krajowych o incydentach

[4] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11.12.2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (Dz.Urz. UE L 321/36 z 17.12.2018).

mających znaczący wpływ na funkcjonowanie sieci lub usług. EKŁE przewiduje również bezpłatne powiadamianie użytkowników o zagrożeniu oraz o możliwych środkach ochronnych lub naprawczych, które użytkownicy mogą podjąć, w przypadkach, w których zagrożenie związane z wystąpieniem incydentu może mieć wpływ na ich sytuację. W art. 41 EKŁE wymaga się, aby właściwe organy krajowe były uprawnione do wydawania wiążących instrukcji w sprawach zapobiegania incydentom lub zaradzenia ich skutkom, w tych przypadkach gdy zidentyfikowano znaczne zagrożenie. Podmioty dostarczające sieci i usługi powinny być zobowiązane do dostarczania informacji niezbędnych do oceny bezpieczeństwa sieci i usług, w tym udokumentowanych polityk bezpieczeństwa oraz poddawania się audytowi bezpieczeństwa. Art. 40 ust. 5 EKŁE przewiduje możliwość przyjmowania przez Komisję Europejską aktów wykonawczych określających szczegółowo techniczne i organizacyjne środki przeciwdziałające zagrożeniom, a także wymagania dotyczące dokonywania zgłoszeń.

W motywie 264 EKŁE wskazano wymagania dotyczące umów pomiędzy dostawcami usług i użytkownikami związane z występowaniem incydentów zagrażających bezpieczeństwu. Umowa powinna precyzować, jaki rodzaj działań dostawca może podjąć w razie wystąpienia zdarzeń naruszających bezpieczeństwo, zagrożenia takimi zdarzeniami lub podatności na wystąpienie takich wydarzeń. Ponadto umowa powinna również precyzować wszelkie ustalenia dotyczące możliwości kompensacji lub zwrotu pieniędzy, jeśli dostawca w nieadekwatny sposób zareaguje na incydent związany z bezpieczeństwem, w tym jeżeli do zgłoszonego dostawcy incydentu związanego z bezpieczeństwem dochodzi z powodu znanych luk bezpieczeństwa w oprogramowaniu lub sprzęcie komputerowym, w związku z czym producent lub programista udostępnił poprawki, a dostawca nie zastosował ich ani nie podjął żadnych innych odpowiednich środków zaradczych.

Specyfika rozwiązań dotyczących cyberbezpieczeństwa w sektorze łączności elektronicznej jest uwzględniana w innych dokumentach unijnych. W marcu 2019 r. Komisja Europejska wydała rekomendacje dotyczące cyberbezpieczeństwa sieci 5G[5]. W styczniu 2020 r. Komisja Europejska opublikowała zalecenie w sprawie wspólnego zestawu środków ograniczających ryzyko w obszarze cyberbezpieczeństwa sieci 5G[6], wypracowane z udziałem ENISA na podstawie danych przekazanych przez państwa członkowskie. Dokument określany jako „5G Toolbox" ma być podstawą do skoordynowanych, wspólnych działań państw UE w zakresie bezpieczeństwa sieci 5G. Dokument zawiera wskazówki dotyczące wymagań w zakresie bezpieczeństwa infrastruktury i usług łączności elektronicznej, oceniania profili ryzyka dostawców, stosowania odpowiednich ograniczeń w odniesieniu do dostawców stwarzających wysokie ryzyko oraz wdrożenia strategii mających na celu zapewnienie dywersyfikacji dostawców. Państwa członkowskie powinny wdrożyć zalecenia do 30 kwietnia i przedstawić sprawozdanie do 30 czerwca 2020 roku.

III. Sektorowe obowiązki w zakresie ochrony bezpieczeństwa sieci i usług

Sektorowe obowiązki przedsiębiorców telekomunikacyjnych w zakresie cyberbezpieczeństwa określają przepisy art. 175–175 e ustawy – Prawo telekomunikacyjne (dalej: pt)[7]. Podstawowym celem ochrony zapewnianej przez przedsiębiorców telekomunikacyjnych ma być bezpieczeństwo

[5] Commission Recommendation of 26.03.2019 Cybersecurity of 5G networks,(C(2019) 2335 final).

[6] Cybersecurity of 5G networks EU Toolbox of risk mitigating measures, https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

[7] Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. DzU 2019, poz. 2460).

i integralność sieci, usług i przekazu komunikatów. Przedmiotem ochrony jest substancja i funkcjonalność sieci oraz jej zdolność do świadczenia usług. Bezpieczeństwo i integralność usług są związane z zachowaniem stabilnych warunków dostarczania usług abonentom przy założonej funkcjonalności usług. W przypadku komunikatów, poza zapobieganiem utracie lub zniekształceniu komunikatu, ochrona ma na celu głównie zabezpieczenie tajemnicy telekomunikacyjnej w odniesieniu do treści komunikatów. Typowe zagrożenia bezpieczeństwa sieci i usług łączności elektronicznej były wielokrotnie przedstawiane w literaturze (Betkier i Górski, 2010, s. 64 i n., Chmielewski i Waćkowski, 2018, s. 85 i n.). Rozbudowane są środki prawno-karne przeciwdziałające tym zagrożeniom (Adamski, 2006, s. 53 i n.)

Podstawowe znaczenie mają środki zapobiegające zagrożeniom dla sieci, usług i komunikatów. Podmiotem zobowiązanym do stosowania środków zabezpieczających sieci, usługi i komunikaty jest dostawca publicznie dostępnych usług telekomunikacyjnych. Ponieważ dostawcy usług mogą świadczyć usługi z wykorzystaniem cudzej infrastruktury, przepis art. 175 ust. 1 pt obciąża tym obowiązkiem także operatora publicznej sieci telekomunikacyjnej, w której prowadzona jest działalność. Przedsiębiorcy telekomunikacyjni są zobowiązani do współdziałania, jeżeli zapewnienie skutecznej ochrony wymaga takiej współpracy. Przedsiębiorca zobowiązany uwzględnia relację między poziomem zagrożeń a nakładami niezbędnymi do ich usunięcia lub ograniczenia. Przedsiębiorca powinien zapewniać poziom bezpieczeństwa odpowiedni do stopnia ryzyka. Ponieważ poziom ryzyka i zagrożeń dla sieci, usług i komunikatów jest zmienny, przedsiębiorca powinien dostosowywać stosowane zabezpieczenia do bieżącej sytuacji. Przedsiębiorca rozważa relację między najnowocześniejszymi osiągnięciami technicznymi w zakresie zabezpieczeń oraz kosztami ich wprowadzenia i dostosowuje środki zabezpieczające do występującego poziomu ryzyka.

Przepis art. 175 pt określa środki zabezpieczające w sposób bardzo ogólny, wskazując jedynie, że są to środki techniczne i organizacyjne. Przewidziano jednak możliwość konkretyzacji tych środków. Zakres stosowanych środków powinien uwzględniać wymagania minimalne wynikające z rozporządzenia wydanego na podstawie art. 175d pt. Dotychczas takie rozporządzenie nie zostało wydane, ale zainicjowano już publiczną konsultację projektu rozporządzenia Ministra Cyfryzacji w tej sprawie[8]. Wymagane środki mają zróżnicowany charakter. Po pierwsze, są to typowe działania organizacyjne, takie jak opracowanie dokumentacji dotyczącej bezpieczeństwa i integralności sieci, ewidencjonowanie infrastruktury i oprogramowania służących do świadczenia usług telekomunikacyjnych, opracowanie zasad i procedur dostępu do kluczowych zasobów systemowych i danych, zabezpieczenie dostępu do kluczowych zasobów infrastruktury telekomunikacyjnej. Po drugie, są to działania przygotowujące przedsiębiorstwo na wystąpienie zagrożeń cyberbezpieczeństwa polegające na identyfikacji zagrożeń poprzez rozpoznanie pojawiających się tendencji, ocenie prawdopodobieństwa wystąpienia tych zagrożeń, dokonywaniu okresowych ocen bezpieczeństwa sieci i usług, zawieraniu umów w powiązaniu z identyfikacją zagrożenia dla sieci i usług, Po trzecie, są to działania zabezpieczające przed negatywnymi następstwami tych zagrożeń, obejmujące m.in. zapewnienie środków minimalizujących skutki ich wystąpienia,

[8] Projekt 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 (z dnia 24 stycznia 20204.) https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/.

zabezpieczenie danych przed nieuprawnionym przetwarzaniem i przygotowanie procedur notyfikacji naruszeń bezpieczeństwa.

Projekt rozporządzenia najbardziej konkretyzuje środki dotyczące sieci 5G, którą identyfikuje się poprzez odesłanie do raportu ETSI TR 121 915 V.15.0.0. (2019-10)[9]. Projekt przewiduje stosowanie przez przedsiębiorców telekomunikacyjnych dostarczających sieci i usługi 5G rekomendacji wydawanych na podstawie uksc, unikanie uzależnienia od jednego producenta poszczególnych elementów sieci oraz podwyższanie odporności na zakłócenia sieci i usług telekomunikacyjnych. Wyraźne podkreślenie wiążącego charakteru rekomendacji wydawanych na podstawie uksc może wywrzeć istotny wpływ na proces doboru partnerów w procesie budowy infrastruktury sieci 5G. Dzięki tym rekomendacjom organy państwowe mogą wpływać na dobór partnerów uczestniczących w budowie sieci rdzeniowej i dostępowej 5G.

IV. Obowiązki informacyjne przedsiębiorców telekomunikacyjnych

1. Obowiązki informacyjne w stosunku do użytkowników usług

Dostawca usług ma obowiązek informowania użytkowników o wystąpieniu szczególnego ryzyka naruszenia bezpieczeństwa sieci, wykraczającego poza zwykły poziom ryzyka i standardowe środki bezpieczeństwa. Jednocześnie, jeżeli istnieją możliwości podniesienia bezpieczeństwa sieci, użytkownicy powinni być o nich poinformowani, a jeżeli podniesienie poziomu bezpieczeństwa wymaga dodatkowych nakładów, użytkownicy powinni być poinformowani o dodatkowych kosztach. Ma to umożliwić użytkownikom dostosowanie poziomu indywidualnych zabezpieczeń do ich potrzeb, związanych z ochroną dostępu do sieci, funkcjonalności usług oraz treści przekazywanej informacji. Przedsiębiorca może odpłatnie oferować dodatkowe środki zabezpieczające.

Szczególna forma informowania użytkowników o zagrożeniach w zakresie cyberbezpieczeństwa polega na publikowaniu informacji o takich zagrożeniach. Przepis art. 175b ust. 2 pt przewiduje, że Urząd Komunikacji Elektronicznej publikuje na stronie internetowej UKE informację o wystąpieniu naruszenia bezpieczeństwa lub integralności sieci lub nakłada na przedsiębiorcę telekomunikacyjnego, w drodze decyzji, obowiązek jej podania do publicznej wiadomości, wskazując sposób jej publikacji, jeżeli uzna, że leży to w interesie publicznym. Decyzji takiej ze względu na charakter sprawy można nadać rygor natychmiastowej wykonalności. Przedsiębiorca wykonuje obowiązek informacyjny na własny koszt. Dotychczas decyzje takie nie były wydawane.

Użytkownicy usług powinni być także poinformowani o działaniach, jakie dostawca usług jest uprawniony podejmować w związku z przypadkami naruszenia bezpieczeństwa lub integralności sieci i usług. Przepis art. 56 ust. 3 pkt 11 lit. f) pt nakazuje zawarcie takich informacji o umowie o świadczeniu usług telekomunikacyjnych. Użytkownikom, którzy zawierają taką umowę poprzez czynności faktyczne (np. użytkownicy usług przedpłaconych) informacje tego rodzaju są przekazywane w regulaminie świadczenia usług telekomunikacyjnych (art. 60 pkt 6 lit. f pt).

Przedsiębiorca telekomunikacyjny został także zobowiązany do partycypowania w informowaniu użytkowników o zagrożeniach w zakresie cyberbezpieczeństwa przez Prezesa UKE. Zgodnie z art. 175e pt Prezes UKE jest zobowiązany do publikowania na swojej stronie internetowej aktualnych informacji o zagrożeniach związanych z korzystaniem z usług, w szczególności

[9] https://www.etsi.org/deliver/etsi_tr/121900_121999/121915/15.00.00_60/tr_121915v150000p.pdf.

o zagrożeniach dla telekomunikacyjnych urządzeń końcowych. W szczególności informacja publikowana na podstawie art. 175e pt powinna obejmować ochronę komputerów i innych urządzeń przetwarzających informacje, pośrednio przyłączonych do sieci telekomunikacyjnej. Typowe informacje publikowane przez Prezesa UKE zawierają ostrzeżenia i wskazówki dotyczące korzystania z usług w instytucjach szczególnie narażonych na ryzyko (np. szkoły, instytucje edukacyjne), korzystania z niektórych funkcji urządzeń końcowych (np. funkcji oddzwaniania na prezentowane numery telefoniczne), korzystania z niektórych uprawnień (np. prawa do „bycia zapomnianym w Internecie"), ryzyka dotyczącego posługiwania się urządzeniami końcowymi (np. ryzyka związanego z kupnem kradzionego telefonu, podmianą karty SIM). Prezes UKE jest zobowiązany do wskazywania potencjalnych zagrożeń związanych z usługami telekomunikacyjnymi. Typowe zagrożenia są związane z korzystaniem z usług o podwyższonej opłacie, wykorzystywaniem usług telekomunikacyjnych do realizacji transakcji finansowych i handlowych, kradzieżą usług telekomunikacyjnych i utratą kontroli nad wysokością należności za wykorzystane usługi. Ponadto, Prezes UKE powinien publikować informacje o najbardziej popularnych sposobach zabezpieczenia urządzeń przed oprogramowaniem złośliwym lub szpiegującym oraz wskazywać konsekwencje nieodpowiedniego zabezpieczenia urządzeń końcowych. Przedsiębiorcy telekomunikacyjni są zobowiązani do współdziałania przy realizacji tej działalności informacyjnej. Przedsiębiorca jest zobowiązany do publikowania informacji przygotowanych przez Prezesa UKE na swojej stronie internetowej. Wykonanie obowiązku informacyjnego jest także możliwe poprzez odesłanie na stronie internetowej przedsiębiorcy do strony Prezesa UKE lub innego podmiotu zajmującego się bezpieczeństwem sieci, gdzie są zamieszczone odpowiednie informacje. Dostawcy usług o większej skali działania prowadzą specjalne strony poświęcone ochronie przed zagrożeniami (np. https://cert.orange.pl/).

2. Obowiązki informacyjne w stosunku do organów państwowych

Przedsiębiorca telekomunikacyjny jest zobowiązany z różnych tytułów do informowania właściwych organów państwowych o wystąpieniu incydentów w zakresie cyberbezpieczeństwa oraz o działaniach podjętych w związku z tymi zagrożeniami.

Przedsiębiorca telekomunikacyjny jest obciążony obowiązkiem informacyjnym dotyczącym zdarzeń polegających na naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miały istotny wpływ na funkcjonowanie sieci lub usług. Obowiązek informacyjny obejmuje jedynie naruszenia mające istotny wpływ na sieci lub usługi. Oceny istotności wpływu dokonuje przedsiębiorca z uwzględnieniem przepisów wykonawczych wydanych na podstawie art. 175a ust. 2a pt. Upoważnienie to zostało zrealizowane rozporządzeniem Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług[10]. Naruszeniem istotnym jest naruszenie, które miało wpływ na co najmniej 10 000 użytkowników i spełnia jeden z warunków dotyczących niedostępności albo ograniczenia dostępności sieci lub usług telekomunikacyjnych przez określony okres liczony w godzinach, w powiązaniu z procentem użytkowników dotkniętych tym wydarzeniem, względnie dotyczy niedostępności połączeń alarmowych w określonej skali. W roku 2017 przekazano Prezesowi UKE informacje o około trzystu

[10] DzU 2018, poz. 1830.

przypadkach naruszeń bezpieczeństwa i integralności sieci i usług, a w roku 2018 odnotowano blisko 200 naruszeń bezpieczeństwa i integralności sieci i usług. Większość z naruszeń miała charakter lokalny (mała skala i krótki czas trwania) i nie wpłynęła w sposób istotny na obsługę klientów telekomunikacyjnych.

Przedsiębiorca powiadamia Prezesa UKE o istotnym naruszeniu, przedstawiając przedmiot tego naruszenia oraz okoliczności związane z jego wystąpieniem. Przedsiębiorca powiadamia również o działaniach zapobiegawczych, czyli działaniach które mają nie dopuścić do wystąpienia podobnego naruszenia w przyszłości. Wreszcie, przedsiębiorca powiadamia o środkach naprawczych, czyli działaniach mających na celu usunięcie skutków naruszenia. Przedsiębiorca ma obowiązek powiadomić Prezesa UKE o standardowych środkach technicznych i organizacyjnych podjętych w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług oraz przekazu komunikatów, a w razie przekazania użytkownikom informacji o środkach ponadstandardowych, również o przekazaniu takiej informacji. Informacje są przekazywane zgodnie z rozporządzeniem Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie wzoru formularza do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług[11]. We wzorze wymaga się wskazania danych identyfikujących przedsiębiorcę, osób uprawnionych do składania Prezesowi UKE wyjaśnień dotyczących zgłaszanych informacji, przedstawienia opisu wpływu naruszenia na usługi oraz przekazania informacji o przyczynie naruszenia, o wpływie naruszenia na kluczowe parametry działalności przedsiębiorcy, a także informacji o podjętych działaniach zapobiegawczych, naprawczych i innych istotnych okolicznościach. Od czerwca 2019 r. UKE umożliwia przekazywanie informacji poprzez Platformę Usług Elektronicznych UKE. Nowa funkcjonalność tej platformy uzupełnia dotychczasowy kanał przesyłania informacji za pomocą poczty elektronicznej poprzez Punkt Kontaktowy Prezesa UKE.

Odrębny obowiązek informacyjny dotyczy podjętych przez przedsiębiorcę telekomunikacyjnego działań w odniesieniu do użytkowników końcowych generujących zagrożenia w zakresie bezpieczeństwa sieci i usług. Na podstawie art. 175c ust. 2 pt przedsiębiorca telekomunikacyjny jest zobowiązany do informowania Prezesa UKE o przypadkach eliminacji przekazu komunikatów zagrażających bezpieczeństwu sieci lub usług albo ich degradacji, a także o ograniczeniu lub przerwaniu świadczenia usługi telekomunikacyjnej w stosunku do zakończenia sieci, z którego wysyłane są takie komunikaty.

Ponieważ funkcjonowanie sieci łączności elektronicznej i świadczenie usług ma kluczowe znaczenie dla całego systemu cyberbezpieczeństwa, przedsiębiorcy telekomunikacyjni są włączeni w system notyfikowania incydentów zagrażających cyberbezpieczeństwu. Ustawa o krajowym systemie cyberbezpieczeństwa zapewniła poprzez nowelizację prawa telekomunikacyjnego mechanizm transmisji informacji o incydentach w zakresie cyberbezpieczeństwa przekazywanych przez przedsiębiorców telekomunikacyjnych. Przepis art. 175a pt powierza Prezesowi UKE obowiązek przekazania niektórych informacji otrzymywanych od przedsiębiorców telekomunikacyjnych do właściwego zespołu reagowania na incydenty bezpieczeństwa komputerowego (CSIRT). Potencjalnie, informacje przekazywane przez przedsiębiorców telekomunikacyjnych mogą trafiać do wszystkich CSIRT przewidzianych ustawą. Ustawa ta powołała na poziomie krajowym CSIRT GOV

[11] DzU 2018, poz. 1831.

prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego, CSIRT MON prowadzony przez Ministra Obrony Narodowej oraz CSIRT NASK prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy. Przekazaniu do właściwego CSIRT podlegają informacje o zdarzeniach będących incydentami w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa, czyli zgodnie z art. 2 pkt 5 tej ustawy – o zdarzeniach, które mają lub mogą mieć niekorzystny wpływ na cyberbezpieczeństwo. Przepis art. 175a ust. 1a pt nakazuje przekazywanie informacji o wszystkich incydentach, które Prezes UKE otrzyma, z tym że otrzymuje on jedynie informacje o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług. Ustalenie, które naruszenia stanowiące incydenty istotne powinny być powodem przekazania informacji, następuje z uwzględnieniem przepisów rozporządzenia wydanego na podstawie art. 175a ust. 2a pt.

Informacja powinna być przekazana do właściwego CSIRT, a właściwość tę należy ustalić na podstawie przepisów art. 26 ust. 5–7 uksc. Przepisy te wskazują, że informacje pochodzące od największych przedsiębiorców telekomunikacyjnych powinny być przekazywane do CSIRT NASK, a niektórych przedsiębiorców do CSIRT MON. Zgodnie z art. 27 ust. 5 pkt 2 CRIRT MON koordynuje obsługę incydentów zgłaszanych przez przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, w stosunku do których organem nadzorującym jest Minister Obrony Narodowej. Wśród tych przedsiębiorców, wymienionych rozporządzeniem Rady Ministrów z 3 listopada 2015 r. w sprawie wykazu przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym[12], którzy są nadzorowani przez MON, są również przedsiębiorcy telekomunikacyjnymi. Większość przedsiębiorców telekomunikacyjnych wymienionych w tym rozporządzeniu podlega jednak nadzorowi ministra właściwego do spraw informatyzacji. Z tego powodu ich informacje o incydentach powinny być kierowane do CSIRT NASK. Prezes UKE nie przekazuje informacji, które na podstawie art. 9 pt zostały zastrzeżone przez przedsiębiorcę jako tajemnica przedsiębiorstwa. Przekazanie informacji powinno nastąpić w postaci elektronicznej, chyba że nie jest to możliwe.

Sektorowy mechanizm informowania o incydentach z zakresu cyberbezpieczeństwa jest zharmonizowany z unijnym systemem gromadzenia danych o takich incydentach. Przepisy art. 175b pt implementują do krajowego porządku prawnego wymóg art. 13a ust. 3 dyrektywy ramowej nakazujący informowanie przez regulatora krajowego innych organów regulacyjnych w państwach członkowskich UE oraz ENISA o naruszeniach bezpieczeństwa sieci i usług. Przedsiębiorcy powinni zgłaszać krajowemu organowi regulacyjnemu naruszenia bezpieczeństwa mające znaczący wpływ na sieci lub usługi, natomiast krajowy organ regulacyjny powinien przekazywać takie informacje innym regulatorom oraz ENISA „w stosownych przypadkach". Przepis art. 175b ust. 1 pt nakazuje przekazanie informacji o naruszeniach, jeżeli Prezes UKE uznaje charakter naruszenia za istotny. Należy jednak przypomnieć, że przedsiębiorcy informują Prezesa UKE o naruszeniach, które miały istotny wpływ na funkcjonowanie sieci lub usług. Mimo podobieństwa sformułowań, ocena istotności naruszenia dokonana przez przedsiębiorcę nie wiąże Prezesa UKE, który samodzielnie dokonuje oceny czy informację o naruszeniu należy przekazać innym regulatorom oraz instytucjom UE. W 2017 roku z ponad trzystu przypadków naruszenia bezpieczeństwa i integralności sieci i usług zgłoszonych Prezesowi UKE, cztery przypadki ze względu na rozległość i czas trwania zostały zakwalifikowane jako istotne, a informacje o nich przekazano do ENISA

[12] DzU poz. 1871 ze zm.

w postaci sformalizowanego raportu[13]. W roku 2018 przekazano do ENISA informacje o dwóch incydentach[14].

Niewykonanie obowiązku zawiadomienia Prezesa UKE o naruszeniu bezpieczeństwa lub integralności sieci lub usług podlega karze pieniężnej na podstawie art. 209 ust. 1 pkt 27[1] pt, który został dodany przepisami uksc. Do czasu tej zmiany kary pieniężne mogły być nakładane na podstawie ogólnego przepisu dotyczącego naruszeń obowiązku informacyjnego w stosunku do Prezesa UKE, czyli art. 209 ust. 1 pkt 1 pt. Wyodrębnienie działu VIIA „Bezpieczeństwo i integralność sieci i usług telekomunikacyjnych" w ustawie – Prawo telekomunikacyjne oraz ustanowienie odrębnej sankcji dotyczącej wykonywania przez przedsiębiorców telekomunikacyjnych obowiązków w zakresie cyberbezpieczeństwa podkreśla znaczenie tych obowiązków dla funkcjonowania sektora telekomunikacyjnego.

V. Obowiązki w zakresie eliminowania zagrożeń dla sieci i usług

Przepisy art. 175c pt, oparte na odpowiednich rozwiązaniach prawa unijnego, stwarzają podstawy do aktywnego przeciwdziałania przez przedsiębiorcę telekomunikacyjnego, pod kontrolą regulatora, zagrożeniom bezpieczeństwa i integralności sieci oraz usług wynikającym z przekazu komunikatów zagrażających tym dobrom. Działanie przedsiębiorcy może prowadzić do eliminacji przekazu komunikatu albo przerwania lub ograniczenia usługi telekomunikacyjnej służącej do wysyłania takich komunikatów. Ponieważ działania takie mogą ograniczać lub pozbawiać użytkowników sieci możliwości komunikowania, muszą być one utrzymane w granicach wynikających z art. 1 ust. 3a dyrektywy ramowej. Zgodnie z tym postanowieniem, państwa członkowskie, stosując środki związane z dostępem użytkowników końcowych do sieci, usług i aplikacji, powinny respektować podstawowe prawa i wolności osób fizycznych gwarantowane w Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności oraz w ogólnych zasadach prawa unijnego. Jeżeli jakikolwiek ze środków związanych z dostępem użytkowników końcowych poprzez sieć do usług i aplikacji mógłby ograniczyć te prawa lub wolności, można go zastosować wyłącznie wtedy, gdy jest odpowiedni, proporcjonalny i konieczny w demokratycznym społeczeństwie, a jego wdrożenie podlega odpowiednim gwarancjom proceduralnym zgodnym z Europejską konwencją i z ogólnymi zasadami prawa wspólnotowego, w tym z zasadą skutecznej ochrony sądowej i zasadą rzetelnego procesu. Środki takie można więc zastosować wyłącznie z należytym poszanowaniem zasady domniemania niewinności i prawa do prywatności. Należy zainteresowanym zagwarantować uprzednią rzetelną i bezstronną procedurę, uwzględniającą prawo wysłuchania, z zastrzeżeniem możliwości potrzeby ustanowienia w pilnych przypadkach odpowiednich warunków oraz zabezpieczeń proceduralnych. Gwarantuje się prawo do skutecznej kontroli sądowej w rozsądnym terminie.

Najbardziej stanowcze środki przeciwdziałania zagrożeniom bezpieczeństwa sieci, usług oraz przekazu komunikatów przewidują przepisy art. 175c pt. Zastosowanie tych środków prowadzi do zaprzestania obsługi telekomunikacyjnej przekazów lub zakończeń sieci generujących zagrożenia. Z tego względu ust. 1 wymaga się, aby ich stosowanie było proporcjonalne i uzasadnione (Piątek, 2019, s. 1228).

[13] Sprawozdanie z działalności Prezesa UKE za 2017 r., https://bip.uke.gov.pl/download/gfx/bip/pl/defaultaktualnosci/24/12/1/sprawozdanie_uke_za_2017.pdf.

[14] Sprawozdanie z działalności Prezesa UKE za 2018 r., bip.uke.gov.pl › bip › 2019_07_04_sprawozdanie_roczne_uke_pl.

Środek o charakterze incydentalnym, przewidziany w art. 175c ust. 1 pkt 1 pt polega na eliminacji przekazu komunikatu. Oznacza to, że przedsiębiorca po rozpoznaniu stanu zagrożenia związanego z konkretnym komunikatem zaprzestaje jego obsługi, w szczególności jego transmisji, przetwarzania lub przechowania, w zależności od rodzaju wykonywanej usługi telekomunikacyjnej. Eliminacja przekazu komunikatu oznacza zaprzestanie wszelkich czynności prowadzących do przekazania komunikatu do zakończenia sieci wskazanego przez nadawcę komunikatu. Środek ten może być zastosowany dopiero po nadaniu komunikatu przez użytkownika. Z art. 175c pt nie wynika obowiązek informowania użytkownika o eliminacji przekazu komunikatu, choć nie ma przeszkód prawnych, aby przedsiębiorca przekazał taką informację użytkownikowi. Może to zapobiec podejmowaniu podobnych działań w przyszłości.

Drugi środek, o charakterze ciągłym, przewidziany w art. 175c ust. 1 pkt 2 pt, polega na przerwaniu lub ograniczeniu świadczenia usługi telekomunikacyjnej na zakończeniu sieci. Środek ten dotyczy usług określonego rodzaju lub wszelkich usług świadczonych dla tego zakończenia sieci. Środek ten można zastosować w razie wysyłania z tego zakończenia komunikatów zagrażających bezpieczeństwu sieci lub usług. Działalność polegająca na wysyłaniu takich komunikatów musi mieć charakter względnie trwały. Przedsiębiorca nie jest zobowiązany do badania czy wysyłanie komunikatów stanowi umyślną działalność użytkownika. Przedsiębiorca nie jest także zobowiązany do wzywania użytkownika, aby zaprzestał wysyłania komunikatów, ale wymóg proporcjonalności i zasadności reakcji przemawia za uprzednim wezwaniem użytkownika do zaprzestania takiej działalności.

Działania wkraczające w możliwości komunikowania przez użytkowników sieci i usług podlegają kontroli Prezesa UKE. Przedsiębiorca jest zobowiązany do niezwłocznego poinformowania Prezesa UKE o zastosowaniu środka eliminującego komunikaty albo przerywającego lub ograniczającego usługę. Informacja powinna zostać przekazana nie później niż w ciągu 24 godzin od podjęcia środka. Przepis art. 175c ust. 2 pt wskazuje główne elementy powiadomienia, które powinno wskazywać zastosowany środek naprawczy oraz zidentyfikowane zagrożenie. Ponadto celowa jest identyfikacja wyeliminowanego komunikatu, zakończenia sieci, którego obsługę przerwano lub ograniczono, a w miarę możliwości identyfikacja użytkownika generującego zagrożenia.

Prezes UKE może w drodze decyzji zakazać stosowania środków wskazanych przez przedsiębiorcę. Przedsiębiorca przywraca obsługę zakończenia sieci oraz nie może blokować przekazu komunikatów, ze względu na te zagrożenia, które zostały zidentyfikowane w związku z podjęciem interwencji. Zakaz stosowania środków powinien być utrzymany w granicach interwencji podjętej przez przedsiębiorcę. Zakaz nie dotyczy zagrożeń bezpieczeństwa lub integralności dla sieci lub usług w związku z wysyłką komunikatów o innym charakterze niż zidentyfikowane w związku z wydaniem decyzji. Podjęcie środków eliminujących przekaz komunikatów lub prowadzących do przerwania lub ograniczenia obsługi w granicach wyznaczonych ustawą uchyla odpowiedzialność przedsiębiorcy za niewykonanie lub nienależyte wykonanie usługi. W przypadku wydania decyzji Prezesa UKE zakazującej stosowania ograniczeń, abonent może dochodzić odpowiedzialności przedsiębiorcy.

VI. Przedsiębiorca telekomunikacyjny jako operator usług kluczowych

Dla oceny statusu przedsiębiorców telekomunikacyjnych w krajowym systemie cyberbezpieczeństwa istotna jest okoliczność, iż przedsiębiorca telekomunikacyjny ze względu na rodzaj

prowadzonej działalności może być jednocześnie operatorem usług kluczowych. Operatorzy tych usług wchodzą w skład krajowego systemu cyberbezpieczeństwa. Wykaz usług kluczowych zawarty w załączniku nr 1 do ustawy obejmuje w sektorze infrastruktura cyfrowa „Podmiot, który świadczy usługi DNS".

Przedsiębiorcy telekomunikacyjni wykorzystują w swojej działalności serwery DNS w celu wykonania usług transmisji danych świadczonych swoim klientom. Ustawa o krajowym systemie cyberbezpieczeństwa nie definiuje pojęć związanych z usługą DNS, natomiast odpowiednie definicje zawiera dyrektywa NIS. Zgodnie z art. 4 pkt 14 dyrektywy NIS „system nazw domen (DNS)" oznacza „hierarchiczny rozproszony system nazw sieciowych, który odpowiada na zapytania o nazwy domen". Natomiast zgodnie z art. 4 pkt 15 tej dyrektywy „dostawca usług DNS" oznacza „podmiot, który świadczy w internecie usługi DNS".

Problem dotyczący zastosowania przepisów o świadczeniu usług DNS do przedsiębiorców telekomunikacyjnych pojawił się już w trakcie prac nad projektem uksc, a następnie w związku z przygotowaniem rozporządzenia przewidzianego w art. 6 uksc. W ramach prac nad projektem ustawy Rada ds. Cyfryzacji wskazywała w uwagach, że „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)". Minister Cyfryzacji wyjaśnił w związku z tym, że „O uznaniu danego podmiotu za operatora usługi kluczowej decydować będą także progi ustalone na mocy art. 6". Problem ponownie pojawił się w pracy nad rozporządzeniem ustalającym te progi. W ramach tych prac wskazywano, że bardzo wiele podmiotów świadczących usługi dostępu do Internetu zapewnia swoim klientom w ramach tej usługi również funkcje oparte na wykorzystaniu własnych serwerów DNS. Izby gospodarcze prowadzące działalność w dziedzinie telekomunikacji wskazywały, że usługi DNS są w praktyce świadczone przez przedsiębiorców telekomunikacyjnych, a sama usługa jest elementem składowym albo towarzyszącym świadczeniu usługi telekomunikacyjnej. W związku z tym postulowano, aby ze względu na zakres i kompleksowość obowiązków dotyczących cyberbezpieczeństwa przewidzianych w ustawie Prawo telekomunikacyjne, wyłączenie z ustawy miało zastosowanie do przedsiębiorców telekomunikacyjnych również w przypadku świadczenia przez przedsiębiorcę telekomunikacyjnego usługi autorytatywnego serwera DNS. Postulat ten został odrzucony przez Ministra Cyfryzacji, który wyjaśnił, że wyłączenie ustawowe dotyczy przedsiębiorców telekomunikacyjnych w zakresie, w jakim są objęci przepisami prawa telekomunikacyjnego. Natomiast podmioty, które będą świadczyć usługi w zakresie DNS mogą zostać uznane za operatora usługi kluczowej niezależnie od tego, że są przedsiębiorcą telekomunikacyjnym.

Kwestia ta była rozpatrywana również na poziomie unijnym w związku z przyjęciem dyrektywy NIS. W załączniku I do Komunikatu Komisji „Pełne wykorzystanie potencjału bezpieczeństwa sieci i informacji – zapewnienie skutecznego wdrożenia dyrektywy (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii"[15] wyjaśniono w punkcie 5.2. przypadek prowadzenia przez przedsiębiorców telekomunikacyjnych m.in. działalności w zakresie DNS. W komunikacie stwierdzono, że wymogi w zakresie bezpieczeństwa i zgłaszania incydentów przewidziane w dyrektywie nie mają zastosowania do dostawców, którzy podlegają wymogom art. 13a i 13b dyrektywy ramowej 2002/21/WE,

[15] COM(2017) 476 final ANNEX 1.

czyli przedsiębiorstw udostępniających publiczne sieci łączności lub świadczących publicznie dostępne usługi łączności elektronicznej. Jeżeli jednak to samo przedsiębiorstwo świadczy również usługi w zakresie DNS, to przedsiębiorstwo takie będzie podlegało wymogom w zakresie bezpieczeństwa i zgłaszania incydentów przewidzianym w dyrektywie NIS. Państwa członkowskie są zobowiązane przeprowadzić proces identyfikacji zgodnie z art. 5 ust. 2 dyrektywy NIS i zidentyfikować tych indywidualnych dostawców usług w zakresie DNS, którzy powinni zostać objęci wymogami dyrektywy NIS, gdyż spełniają kryteria przewidziane w art. 5 ust. 2 tej dyrektywy.

Z powyższego wynika, że przedsiębiorcy telekomunikacyjni nie są automatycznie wyłączeni z zakresu zastosowania dyrektywy NIS, a w konsekwencji z zakresu stosowania ustawy o cyberbezpieczeństwie, jeżeli świadczą usługi DNS w zakresie określonym dyrektywą NIS i przepisami krajowymi. Dlatego w każdym przypadku konieczne jest dokonanie oceny czy przedsiębiorca jest „podmiotem, który świadczy usługi DNS" w rozumieniu uksc, z uwzględnieniem znaczeń nadanych poszczególnym pojęciom w dyrektywie NIS.

Z powołanych wyżej krajowych i unijnych aktów prawnych wynika, że wykorzystanie infrastruktury DNS może następować w ramach działalności przedsiębiorcy telekomunikacyjnego, jako element składowy usługi telekomunikacyjnej (usługi łączności elektronicznej). Wykorzystanie serwerów DNS przez przedsiębiorcę telekomunikacyjnego w ramach własnej działalności polegającej na świadczeniu usług telekomunikacyjnych nie stanowi świadczenia usługi DNS. Informacje o naruszeniach bezpieczeństwa usług i sieci telekomunikacyjnych, które stanowią incydenty w odniesieniu do infrastruktury DNS eksploatowanej przez przedsiębiorcę telekomunikacyjnego są przekazywane Prezesowi UKE, który przesyła je do właściwego CSIRT na zasadach określonych ustawą – Prawo telekomunikacyjne.

Przedsiębiorca telekomunikacyjny może jednak, poza swoją podstawową działalnością polegającą na dostarczaniu sieci i świadczeniu usług telekomunikacyjnych, świadczyć również odrębnie usługę DNS. Przedsiębiorca telekomunikacyjnych jest w takim przypadku również dostawcą usług DNS. Z dyrektywy wynika, że powinno to być świadczenie samodzielne, zapewniane niezależnie od usługi telekomunikacyjnej. Usługi tego rodzaju są świadczone i odrębnie rozliczane przez dostawców, na przykład na podstawie liczby obsłużonych zapytań. W świetle przepisów uksc oraz dyrektywy NIS może zatem wystąpić sytuacja, w której przedsiębiorca jest jednocześnie przedsiębiorcą telekomunikacyjnym oraz dostawcą usług DNS. Podmiot taki nie staje się jednak dostawcą usług DNS tylko z tego powodu, że w ramach działalności telekomunikacyjnej zapewnia swoim abonentom obsługę funkcji DNS za pomocą własnej infrastruktury. W konsekwencji, załącznik nr 1 do uksc w części dotyczącej „podmiotu, który świadczy usługi DNS" nie obejmuje przedsiębiorców telekomunikacyjnych, którzy zapewniają funkcję DNS tylko swoim abonentom.

Ocena dotycząca zastosowania przepisów uksc w zakresie świadczenia usługi DNS musi również uwzględnić przepisy rozporządzenia Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych[16]. Rozporządzenie to w odniesieniu do podmiotu, który świadczy usługi DNS określa usługę kluczową jako „Prowadzenie autorytatywnego serwera DNS", a próg istotności skutku zakłócającego incydentu dla świadczenia usługi kluczowej jako „minimalnie 100 tys. nazw domen, dla których serwer jest autorytatywny". Prowadzenie serwera autorytatywnego dotyczy

[16] DzU 2018, poz. 1806.

domeny w strefie, nad którą dany serwer ma zarząd, a odpowiedzi na zapytania pochodzą bezpośrednio z bazy danych serwera. Odpowiedź przekazywana przez taki serwer wskazuje, że została uzyskana z serwera dokonującego bezpośredniego uwierzytelnienia poszukiwanej nazwy. Na podstawie art. 5 uksc oraz rozporządzenia w sprawie progów organ właściwy do spraw cyberbezpieczeństwa będzie wydawał decyzje o uznaniu określonego podmiotu za operatora usługi kluczowej. Ostatecznie zatem, o zaliczeniu konkretnego podmiotu do kategorii dostawców usług DNS przesądzi decyzja administracyjna.

W związku ze wskazanymi wyżej przepisami należy uznać, iż jeżeli przedsiębiorca telekomunikacyjny obok zapewniania funkcji DNS swoim abonentom, świadczy dodatkowo w Internecie usługę DNS spełniającą wymagania określone rozporządzeniem (autorytatywny charakter informacji DNS) oraz przekraczającą próg określony rozporządzeniem (minimalnie 100 tys. domen), to taka działalność powinna być uznana za świadczenie usługi kluczowej i przedsiębiorca telekomunikacyjny świadczący taką usługę będzie podlegał przepisom uksc niezależnie od tego, że do jego działalności w zakresie świadczenia usług telekomunikacyjnych będą miały zastosowanie przepisy art. 175–175e prawa telekomunikacyjnego (Besiekierska, 2019, art. 1, Nb. 11). Potwierdza to stanowisko Ministerstwa Cyfryzacji, które stwierdza w przypadku, gdy przedsiębiorca telekomunikacyjny zostanie uznany za operatora usługi kluczowej w sektorze infrastruktury cyfrowej, wówczas będzie podlegał regulacjom uksc. Uznanie przedsiębiorstwa telekomunikacyjnego za operatora usługi kluczowej w rozumieniu uksc, pociąga za sobą realizację obowiązków wynikających z tej ustawy w całej rozciągłości (w tym także w odniesieniu do wymogów dotyczących bezpieczeństwa i zgłaszania incydentów w zakresie świadczonej usługi kluczowej)[17]. Należy podzielić wyrażony w literaturze pogląd, iż dyrektywa NIS nie miała na celu uszczegółowienia przepisów dotyczących sieci i usług łączności elektronicznej, lecz objęcie regulacjami w zakresie cyberbezpieczeństwa grupy innych podmiotów, mających istotne znaczenie z uwagi na świadczone usługi lub posiadaną infrastrukturę (Rojszczak, 2018, s. 206). W praktyce podmioty te mogą jednocześnie prowadzić działalność w zakresie dostarczania sieci i usług telekomunikacyjnych.

Bibliografia

Adamski, A. (2006). Cyberprzestępczość – aspekty prawne i kryminologiczne. *Studia Prawnicze*, (4).

Besiekierska, A. (red.). (2019). *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*. Warszawa: Wydawnictwo C.H. Beck.

Betkier, M. i Górski, J. (2010). Ochrona sieci przed zagrożeniami. *Prawo i Regulacje Świata Telekomunikacji i Mediów*, (2).

Chmielewski, J.M. i Waćkowski, K. (2018). Technologie informatyczne – podstawy, rozwój i bezpieczeństwo systemów teleinformatycznych. W: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*. Warszawa: Wolters Kluwer.

Kitler, W., Taczkowska-Olszewska, J. i Radoniewicz F. (red.). (2019). *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*. Warszawa: Wydawnictwo C.H. Beck.

Piątek, S. (2019). *Prawo telekomunikacyjne. Komentarz*. Warszawa: Wydawnictwo C.H. Beck.

Rojszczak, M. (2018). Cyberbezpieczeństwo w łączności elektronicznej. W: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*. Warszawa: Wolters Kluwer.

[17] https://www.gov.pl/web/cyfryzacja/operatorzy-uslug-kluczowych.