



KRAJOWA IZBA KOMUNIKACJI ETHERNETOWEJ

ul. Lindleya 16

02-013 Warszawa

Tel. + 48 22 29 28 700, Fax +48 22 29 28 701

e-mail: biuro@kike.pl, grap@kike.pl, <http://www.kike.pl>

KRS 0000316678, REGON: 141637224, NIP 9512270210

Warszawa, dnia 2 czerwca 2017 roku

ID KIKE: GRAP 292/17

Szanowny Pan

Wiesław Janczyk

Sekretarz Stanu w Ministerstwie Finansów

ul. Świętokrzyska 12

00-916 Warszawa

Dotyczy: obowiązków przedsiębiorców telekomunikacyjnych w związku z Rejestrem Domen Zakazanych

Szanowny Panie Ministrze,

Wykonana przez nas analiza art. 15f ust. 5 ustawy z dnia 19 listopada 2009 r. o grach hazardowych (ustawa hazardowa) przeprowadzona w kontekście mechanizmu translacji nazw domenowych na adresy IP realizowanego przez serwery DNS (Domain Name System) wskazuje, iż od strony technicznej realizacja wskazanych w ustawie celów możliwa jest wyłącznie w dwóch sferach:

1. Na serwerach rejestratorów domen, na których możliwe jest **usunięcie** wpisów wskazanych w RDZ;
2. Na serwerach DNS podmiotów zobowiązanych poprzez **przekierowanie** zapytań do domen wskazanych w RDZ na adres wskazany przez MF.

Mając na uwadze powyższą analizę przedkładamy poniższe pytania oraz propozycje usprawnienia wdrażania wskazanych w ustawie hazardowej wymagań.

Analizując rynek telekomunikacyjny chcielibyśmy zwrócić uwagę Pana Ministra, że zgodnie z raportem Audytela¹, sporządzonym na zlecenie Ministerstwa Cyfryzacji, **blisko 60% małych i średnich przedsiębiorstw telekomunikacyjnych (MŚP) nie obsługuje więcej niż 300 abonentów, zaś 80% nie ma 1000 abonentów.** Niewielka skala prowadzonej działalności wiąże się z kilkoma charakterystycznymi problemami, z których najważniejszym jest fakt, iż podmioty te nie posiadają własnych serwerów DNS umożliwiających realizację przekierowań wskazanych w pkt 2 powyżej. Problem ten poruszamy poniżej. Jednak równocześnie należy wskazać, iż zgodnie z w/w Raportem Audytela – udział MŚP w rynku wynosi blisko 30%. Krajowa Izba Komunikacji Ethernetowej (**KIKE**) reprezentując operatorów z segmentu MŚP uprzejmie prosi Pana Ministra o wyjaśnienie wątpliwości w odniesieniu do zakresu podmiotowego art. 15f ust. 5 pkt 1 i 2 ustawy hazardowej, który wchodzi w życie 1 lipca br. Wyjaśnienie zakresu i prawidłowej realizacji obowiązków określonych w art. 15f ust. 5 pkt 1 i 2 ustawy hazardowej powinno rozwiązać wszelkie wątpliwości związane ze stosowaniem jej art. 15f ust. 5 pkt 3, ponieważ przepis ten stanowi odwrócenie obowiązków ujętych w art. 15f ust. 5 pkt 1 i 2. Prosimy o rozważenie wydania wytycznych określających właściwy **sposób realizacji obowiązków** ujętych w tym przepisie, tym bardziej, że w ustawie nie przewidziano możliwości wydania rozporządzenia wykonawczego.

Przed dalszymi rozważaniami należy przypomnieć, że na mocy art. 15f ust. 5 ustawy hazardowej **przedsiębiorcy telekomunikacyjni** świadczący usługi **dostępu do sieci** Internet będą obowiązani do:

- 1) uniemożliwienia dostępu do stron internetowych wykorzystujących nazwy domen wpisanych do Rejestru Domen Zakazanych (RDZ) poprzez ich **usunięcie** z systemów teleinformatycznych przedsiębiorców telekomunikacyjnych, służących do zamiany nazw domen internetowych na adresy IP,
- 2) **przekierowania** połączeń odwołujących się do nazw domen internetowych wpisanych do RDZ do strony internetowej zawierającej odpowiedni komunikat,
- 3) umożliwienia dostępu do stron internetowych wykorzystujących nazwy domen wykreślonych z RDZ, nie później niż w ciągu 48 godzin od wykreślenia nazwy domeny internetowej z RDZ.

Podstawowym zagadnieniem jest więc wyjaśnienie **podmiotowego zakresu obowiązków** określonych w art. 15f ust. 5 ustawy hazardowej. W opinii KIKE formalnie obowiązek ten formułowany jest wobec operatorów w rozumieniu ustawy – Prawo telekomunikacyjne (Pt), zarządzających własnymi serwerami **DNS**. Tymczasem, ze swej istoty

¹ https://mc.gov.pl/files/raport_dla_mac_inwestycje_msp_w_sieci_szerokopasmowe_audytelem_2016-10-30j_na_czysto.pdf - str. 8.

obowiązek, o którym mowa w art. 15f ust. 5 pkt 1 ustawy hazardowej może być skutecznie zrealizowany wyłącznie przez podmioty zwane 'DNS Registrars', które najczęściej nie są przedsiębiorcami telekomunikacyjnymi, a zatem obecna ustawa nie nakłada na nich, jak się wydaje, żadnych obowiązków. **Jednak w praktyce funkcjonowania serwerów DNS tylko te podmioty mogą globalnie i skutecznie usunąć lub zablokować oryginalne wpisy w bazach danych zarejestrowanych domen.**

Dla MŚP niezwykle istotna jest również odpowiedź na pytanie, **czy i jakie obowiązki spoczywają na operatorach, którzy nie dysponują własnymi serwerami DNS?**

Apelujemy przy tym o współpracę Ministerstwa Finansów z Urzędem Komunikacji Elektronicznej oraz pozostałych podmiotów wskazanych w rozdzielniku niniejszego pisma, które dysponują szeroką wiedzą i doświadczeniem w dziedzinie telekomunikacji. Ze swojej strony, jeżeli powstanie taka potrzeba, również **oferujemy wszelką możliwą pomoc i współpracę**, w tym w ewentualnym opracowaniu stosownych procedur i szczegółowych przykładów konfiguracji serwerów DNS.

I. Wątpliwości dotyczące art. 15f ust. 5 (część wspólna) ustawy hazardowej

Już na etapie wykładni językowej części wspólnej art. 15f ust. 5 ustawy można mieć wątpliwości, na kim spoczywają obowiązki określone w tym przepisie. „Przedsiębiorca telekomunikacyjny” (art. 2 pkt 27 Pt) jest podmiotem wykonującym działalność gospodarczą polegającą na dostarczaniu sieci telekomunikacyjnych, świadczeniu usług towarzyszących lub świadczeniu usług telekomunikacyjnych. **Nie każdy przedsiębiorca świadczący usługi telekomunikacyjne jest właścicielem sieci telekomunikacyjnej, w której świadczy usługi telekomunikacyjne.** Niektórzy przedsiębiorcy świadczą usługi telekomunikacyjne z wykorzystaniem sieci dostarczanej przez innego przedsiębiorcę – operatora. Jest to model usług świadczonych przez tzw. „Operatorów Alternatywnych” (OA) lub wirtualnych, powszechny i znany np. na gruncie operatorów telefonii komórkowej. Przedsiębiorca telekomunikacyjny, uprawniony do świadczenia usług telekomunikacyjnych, zwany jest „dostawcą usług” (art. 2 pkt 27 lit. a Pt), a przedsiębiorca uprawniony do dostarczania publicznych sieci telekomunikacyjnych lub świadczenia usług towarzyszących, zwany jest „operatorem” (art. 2 pkt 27 lit. b Pt). Korzystanie z sieci innego przedsiębiorcy (operatora) wymaga m.in. **dostępu do sieci telekomunikacyjnej** (pojęcie „dostępu telekomunikacyjnego”, który obejmuje dostęp do sieci, jest zdefiniowane w art. 2 pkt 6 Pt). Świadczenie usług telekomunikacyjnych na sieci operatora trzeciego może być realizowane jednak zarówno w modelu:

- zakupu kompletnej usługi IP od właściciela sieci telekomunikacyjnej (np. tutaj komplet usługi zapewnia dawca sieci, a usługodawca realizuje w praktyce głównie rozliczenia i zapewnia wsparcie klienta);

- jak i różnych wariantów dostępu hurtowych (np. Local Loop Unbundling, czy Bit Stream Access), w których to usługodawca, a nie operator sieci, zapewnia realizację usług na poziomie IP (od warstwy 3 modelu OSI).

Równocześnie zaznaczyć bowiem należy, iż coraz powszechniej na rynku realizowane jest udostępnienie przez tzw. Operatorów Infrastruktury (dalej **OI**) własnej lub dzierżawionej infrastruktury telekomunikacyjnej usługodawcom trzecim (OA). Część OI nie świadczy przy tym żadnych usług IP, w szczególności usług detalicznych. Nie mają oni więc żadnej możliwości limitowania dostępu do stron wskazanych w RDZ.

W świetle powyższych definicji, nie sposób z całą pewnością przesądzić, kiedy obowiązki określone dla „przedsiębiorców telekomunikacyjnych świadczących usługi **dostępu do sieci Internet**” spoczywają na dostawcach usług, a kiedy na właścicielach lub dzierżawcach, którzy zapewniają dostęp do sieci. Rozstrzygnięcie tej kwestii ma duże znaczenie, ponieważ wyznacza **krąg podmiotów, na których spoczywa obowiązek** określony w ustawie.

W opinii KIKE zasadne jest, aby z powodów technicznej możliwości realizacji obowiązki przewidziane w art. 15f ust. 5 i adresowane do przedsiębiorców telekomunikacyjnych **spoczywały wyłącznie na podmiotach zapewniających klientowi adresację IP**, ponieważ tylko te podmioty zapewniają klientom końcowym usługi (na sieci własnej lub cudzej) oparte o IP. Dostawca np. pętli abonenckiej w modelu LLU nie ma bowiem żadnego wpływu na komunikację abonenta końcowego z serwerami DNS, a to modyfikacji na serwerach DNS dotyczy omawiana dyspozycja ustawowa. Pamiętać jednak nadal należy o w/w przypadku, w którym formalny dostawca usług korzysta w praktyce z usługi (w uproszczeniu adresacji) innego operatora. W tym przypadku jest on w całości uzależniony od konfiguracji sieci operatora trzeciego odpowiadającego infrastrukturalnie za dostarczenie usługi IP klientowi końcowemu.

W tym miejscu należy również postawić pytanie, czy operatorzy są zobowiązani do obsługi RDZ na łączach międzyoperatorskich np. **IP Transit** (łącza realizujące transmisję ruchu w sieci pomiędzy innymi operatorami), gdy odbiorcą ruchu jest inny operator? Podobne wątpliwości towarzyszą sytuacji, gdy pośrednikiem ruchu jest członek węzła wymiany ruchu między operatorami (np. węzły IX – ang. Internet eXchange), który nie jest wpisany do rejestru przedsiębiorców telekomunikacyjnych.

Zdaniem KIKE obowiązki określone w art. 15f ust. 5 ustawy hazardowej powinny spoczywać na operatorach wyłącznie wówczas, gdy połączenie zestawiane jest bezpośrednio do danego klienta (użytkownika końcowego w rozumieniu Pt) z uwzględnieniem w/w rozważań dot. podmiotu udostępniającego abonentowi adres IP i usługę dostępu do własnych serwerów DNS.

II. Wątpliwości dotyczące art. 15f ust. 5 pkt 1 ustawy hazardowej

Zamianę nazw domen na adresy IP umożliwiają serwery DNS. Przepis art. 15f ust. 5 pkt 1 ustawy wymaga uniemożliwienia dostępu do domen wpisanych do RDZ „poprzez ich **usunięcie** z systemów teleinformatycznych przedsiębiorców telekomunikacyjnych, służących do zamiany nazw domen internetowych na adresy IP”, czyli (jak można przypuszczać) z serwerów DNS. Chcemy jednakże zwrócić uwagę Pana Ministra na to, że w uproszczeniu istnieją **dwa typy serwerów DNS**.

Pierwszy typ, to serwery DNS na których rejestrowane są domeny i które zawierają dane źródłowe. Jak już wspomnieliśmy wyżej, w zasadzie tylko na nich można **usunąć** nazwę domenową umieszczoną w RDZ. Domeny rejestruje się bowiem na nadrzędnych serwerach prowadzonych przez tzw. ‘DNS Registrars’. Przykładowo dla większości polskich domen (*.pl) obowiązki takie realizuje m.in. Naukowa i Akademicka Sieć Komputerowa. NASK jest tylko **jednym z wielu** tego typu podmiotów rejestrujących domeny. Każda domena jest jednak zarejestrowana u konkretnego ‘Registrara’ i tylko u niego znajduje się pierwotny wpis, do którego odnoszą się pośrednio wszyscy użytkownicy Internetu wywołujący daną nazwę. Tylko u źródła więc można skutecznie usunąć („z Internetu”) nazwę wskazaną w RDZ. ‘Rejestrar DNS’ rezerwują daną domenę dla określonego podmiotu i przechowują informację o domenie i przypisanym do niej adresie IP tak długo, jak długo dany podmiot opłaca utrzymanie zarejestrowanej domeny.

Serwery DNS operatorów telekomunikacyjnych (jeśli dany operator posiada własne serwery DNS, co nie jest częste) służą co do zasady do innego celu i działają odmiennie. W praktyce są usługami typu *cache* lub *proxy*. Otrzymując zapytanie o daną domenę od klienta, serwery DNS operatorów kontaktują się z serwerami nadrzędnymi DNS w Internecie, aż dotrą do serwera, z którego otrzymają źródłową informację o tym, skąd pobrać szczegółowe informacje na temat poszukiwanej domeny, a następnie jaki adres IP jest jej przypisany. Informację uzyskaną od serwerów nadrzędnych serwer DNS cache przesyła następnie do komputera klienta. Serwer DNS cache operatora pełni więc rolę pośrednika działającego na żądanie. **Taki serwer pośredniczący jedynie tymczasowo umieszcza w swoim buforze odpowiedzi na zapytania klientów**, aby usprawnić (przyspieszyć) obsługę powtarzających się zapytań do typowych domen, **ale w żadnym przypadku nie utrzymuje rejestru domen w sieci** (nie jest ‘DNS Registrarem’). Wręcz przeciwnie – w plikach tymczasowych dysponuje bardzo ograniczonym zasobem informacji o bieżących zapytaniach. Serwer lokalny DNS operatora, co do zasady, nie jest też źródłem informacji dla innych serwerów DNS. W związku z tym usunięcie domen z tych serwerów nie przyniosłoby żadnego skutku w dostępie do zabronionej domeny poprzez inne serwery DNS.

W tym miejscu należy wskazać z całą mocą, iż **nie istnieje żadna techniczna możliwość, by zablokować klientom jakiegokolwiek sieci dostęp do dowolnego z dostępnych w**

Internecie serwerów DNS². Istnieje bowiem co najmniej kilkanaście sposobów na obejście wszelkich blokad lub przekierowań możliwych do zaprojektowania w sieci operatora telekomunikacyjnego, choćby wykorzystując najprostsze połączenia VPN, czy darmowe oprogramowanie dostępne do sieci Tor, którego instalacja zajmuje kilkanaście sekund i nie wymaga żadnej wiedzy informatycznej.

W związku z powyższym, **usunięcie nazw domen** z serwerów DNS, które miałyby skutecznie „uniemożliwić dostęp do stron internetowych wykorzystujących nazwy domen wpisanych do RDZ”, **możliwe byłoby wyłącznie poprzez usunięcie ich z serwerów DNS Registrars**, na których domeny te zostały zarejestrowane, lub w szczególnych przypadkach (gdy tzw. pliki stref umieszczone są poza serwerami podmiotów rejestrujących) na źródłowym serwerze DNS firmy rejestrującej. **Nie zaś u operatora**, który korzysta z serwera DNS cache, które jedynie przyspieszają zestawienie połączenia do często używanych witryn, a wszelkie dane potrzebne do tego zestawienia przechowują jedynie tymczasowo w swoim buforze.

Tymczasem prowadzenie rejestrów i przechowywanie danych (w tym plików stref domen) nie jest dostarczaniem sieci, ani usługą towarzyszącą (zdefiniowaną w art. 2 pkt 44a Pt), ani usługą telekomunikacyjną (która polega głównie na przekazywaniu sygnałów w sieci telekomunikacyjnej – art. 2 pkt 48 Pt). W związku z powyższym prowadzenie DNS Registry **nie jest usługą, którą dany podmiot świadczy jako przedsiębiorca telekomunikacyjny**.

W związku z powyższym nie mamy pewności, **czy art. 15f ust. 5 pkt 1 ustawy hazardowej nakłada realny obowiązek na jakikolwiek podmiot**, choć jednoznacznym jest, iż jedynie takie rozwiązanie umożliwia **usunięcie** domeny wpisanej do RDZ.

Niezależnie od powyższego, zakres obowiązku określonego w art. 15f ust. 5 pkt 1 ustawy jest również niejasny w świetle kolejnego obowiązku, o którym mowa w art. 15f ust. 5 pkt 2 ustawy. Zgodnie z art. 15f ust. 5 pkt 2 ustawy przedsiębiorcy telekomunikacyjni „świadczący usługi dostępu do sieci Internet” powinni przekierowywać połączenia odwołujące się do nazw domen internetowych wpisanych do RDZ do strony internetowej zawierającej odpowiedni komunikat. Obowiązki z art. 15f ust. 5 pkt 1 i pkt 2 **wydają się wzajemnie sprzeczne**, ponieważ usunięcie nazwy domeny z serwera DNS powoduje, że nie sposób jednocześnie połączeń z tą domeną przekierowywać. Przekierowanie wymaga wprowadzenia odpowiedniej reguły (wpisu) w systemie operatora. Jeśli zdecydujemy się na usunięcie, w praktyce abonent zamiast przekierowania przeglądarki na stronę MF, otrzymałby komunikat, że dana domena nie istnieje³.

W związku z powyższym należy rozważyć zmianę ustawy w taki sposób, aby art. 15f ust. 5 pkt 1 ustawy hazardowej nakładał obowiązki na DNS Registrars – przynajmniej tych, których działalność zlokalizowana jest na terytorium Polski – a nie na przedsiębiorców

² Jeśli istnieje sposób na ingerencję w połączenia realizowane za pomocą protokołów VPN, prosimy o przykłady konfiguracji routerów pośredniczących.

³ Przykładowy komunikat, gdy nie ma wpisu o danej domenie lub został on usunięty: „Nie udało się znaleźć adresu DNS serwera **szukanastronahazardowa.com**”.

telekomunikacyjnych. Lub też odstąpić od zapisów odnoszących się do obowiązku **usuwania** domen wskazanych w RDZ.

III. Wątpliwości dotyczące art. 15f ust. 5 pkt 2 ustawy hazardowej

Charakterystyka serwerów DNS, którymi posługują się operatorzy telekomunikacyjnych rodzi pytanie, co może zrobić operator telekomunikacyjny, aby realizować obowiązek określony w art. 15f ust. 5 pkt 2 ustawy hazardowej? Operator może oczywiście otrzymując zapytanie od abonenta wskazać jako cel nie właściwe IP uzyskane z serwerów nadrzędnych, a inne IP wpisane „statycznie” w konfiguracji własnego, lokalnego serwera DNS – w omawianym przypadku adres strony zawierającej odpowiedni komunikat. Proces ten, to w praktyce przekierowywanie połączeń odnoszących się do zakazanych domen do innej strony internetowej. Jednak realizacja tego zadania wobec wszystkich swoich abonentów przez operatora telekomunikacyjnego nie zawsze jest możliwa. Powody są przede wszystkim dwa:

1. **Nie wszyscy abonenci korzystają z serwerów DNS swojego operatora/dostawcy** Internetu nawet, jeśli on taką usługę realizuje. Abonent może korzystać w zasadzie z dowolnego serwera DNS w sieci, także zlokalizowanego poza granicami Polski. Bardzo typowe jest wykorzystywanie publicznego serwera DNS Google o popularnym adresie IP: 8.8.8.8.
2. Duża część mniejszych operatorów **nie ma zaś własnych serwerów DNS**, na których mogłaby technicznie zrealizować ten obowiązek. Co do zasady posiadanie własnych serwerów DNS nie jest obowiązkowe, ani niezbędne do świadczenia usługi dostępu do sieci Internet i ma uzasadnienie co do zasady wyłącznie w większych sieciach oraz u operatorów rejestrujących domeny własne lub swoich klientów.

Powyższe ograniczenia powodują, iż mniejsi operatorzy, w tym podmioty zrzeszone w KIKE, borykają się z szeregiem wątpliwości jak zapewnić prawidłową realizację nałożonych na nich obowiązków?

Ad. 1. Swobodny wybór serwera DNS

W odniesieniu do serwerów DNS należy wskazać, że duża część klientów operatorów telekomunikacyjnych korzysta z innych serwerów DNS, niż serwer własnego dostawcy Internetu.

W opinii KIKE obowiązek określony w art. 15f ust. 5 pkt 2 ustawy hazardowej spoczywa na operatorze wyłącznie w zakresie konfiguracji własnego serwera DNS. Obowiązek ten powinien polegać na ustanowieniu **przekierowania** wszystkich połączeń z domenami ujętymi w RDZ na stronę MF z odpowiednim komunikatem. W przypadku jednak, gdy **klient danego**

operatora korzysta z innego serwera DNS, niż serwer tego operatora, operator nie powinien ingerować w wybór klienta odnośnie korzystania z obcego serwera DNS.

W przypadku jednak, gdyby Pan Minister skłaniał się do innego stanowiska, należy podkreślić, że jak wspomnieliśmy już wyżej **nie ma technicznej możliwości skutecznego przechwytywania wszystkich zapytań klientów dotyczące wyłącznie wybranych domen.** Ewentualne przechwytywanie wszystkich zapytań każdego klienta na porcie UDP 53 (wszystkie próby połączenia się przez każdego klienta z dowolną stroną www) celem zapewnienia przekierowania na stronę MF z komunikatem nie jest możliwe technicznie do zrealizowania. Niezależnie od niewyobrażalnie wysokich kosztów filtrowania całego ruchu szerokopasmowego w warstwie 4 lub 3, istnieje zbyt wiele sposobów, by obejść jakiegokolwiek filtry, jakie mogliby teoretycznie uruchomić operatorzy. Oznaczałoby to ponadto ograniczenie dostępu do otwartego Internetu i zakazu ingerowania w treść transmisji. W praktyce też podobne rozwiązania oznaczałyby faktyczne monitorowanie wszelkich zapytań każdego z klientów, co zbliża się już niebezpiecznie do naruszenia regulacji o ochronie prywatności. Takie przechwytywanie tworzyłoby furtkę do analizy wszystkich stron, z których korzystają poszczególni klienci,

Izba czuje się zobowiązana do wskazania, że właściwą praktyką operatorów w kontekście zapisów ustawy hazardowej jest przygotowanie i udostępnienie klientom serwera DNS realizującego przekierowania na stronę z odpowiednim komunikatem.

Ad. 2. Brak własnego serwera DNS

Biorąc pod uwagę, że zgodnie z przytoczonym na wstępie raportem Audytela blisko 60% MŚP nie obsługuje więcej niż 300 abonentów, istnieje duże prawdopodobieństwo, że wręcz żaden z przedsiębiorców tej wielkości nie posiada własnych serwerów DNS. Najważniejsze pytanie dla tych podmiotów brzmi zatem, jakie obowiązki na nich ciążą?

W przekonaniu KIKE ustawa hazardowa **nie nakłada na takich przedsiębiorców żadnych obowiązków**, gdyż ich realizacja możliwa jest na własnym serwerze DNS.

W przypadku, gdyby Pan Minister nie podzielał tego poglądu, niezwykle ważne byłoby dla nas uzyskanie wskazówek dotyczących kwestii, **w jaki sposób operatorzy nieposiadający własnych serwerów DNS powinni realizować przekierowania.** Z tym pytaniem wiąże się kilka bardziej szczegółowych pytań:

- 1) Czy na lokalnych operatorach Internetu, których abonenci korzystają z obcych serwerów DNS (z braku własnych), ciąży obowiązek przekierowywania dostępu do domen wpisanych do RDZ na stronę z komunikatem? Czy też odpowiedzialność ta spoczywa w całości na operatorach nadrzędnych?
- 2) Czy planowane jest uruchomienie przez MF, NASK, UKE lub inną jednostkę publiczną referencyjnego serwera DNS dla małych operatorów nie posiadających własnych serwerów DNS, do których mogłyby być kierowane połączenia

abonentów, aby zabezpieczyć blokowanie dostępu do nazw domen wpisanych do rejestru?

- 3) Wielu najmniejszych operatorów nie dysponuje również pulą własnych adresów IP, lecz działa w oparciu o adresy operatora nadrzędnego – tzw. adresy ‘Provider Aggregatable – PA’. Czy operator lokalny wykorzystujący całkowicie zależne od dostawcy nadrzędnego adresy PA (nie korzystając samodzielnie z Border Gateway Protocol – BGP) ma obowiązek niezależnie od swojego dostawcy realizować przekierowania na stronę z komunikatem – w praktyce powielając mechanizm implementowany już przez operatora nadrzędnego? Czy też ten obowiązek leży jedynie po stronie operatora nadrzędnego – dawcy adresacji PA?

IV. Propozycja rozszerzenia katalogu plików zawierających RDZ

RDZ udostępniany jest obecnie w formacie pliku XML, którego implementacja na popularnych serwerach DNS wymaga zastosowania dodatkowego oprogramowania konwertującego dane do formatów wymaganych przez serwery DNS. Fakt ten oznacza, iż wdrożenie ustawy hazardowej wymaga wiedzy i zastosowania dodatkowych narzędzi, które będą przetwarzać plik XML do formatu wykorzystywanego przez serwery DNS.

Krajowa Izba Komunikacji Ethernetowej wnioskuje, by Ministerstwo Finansów równoległe z plikiem XML publikowało pliki gotowe do implementacji na serwerach DNS/DNS Proxy.

I tak:

1. Bazując na bieżących wpisach do RDZ, gotowy plik strefy dla najpopularniejszego obecnie serwera DNS o nazwie Bind, wyglądać mógłby następująco:

```
## 30-05-2017 19:02:54
```

```
zone "www.slbet.com" { type master; file "/etc/bind/db.hazard-redirect"; }; # dodano: 2017-05-26T08:53:41
```

```
zone "betcris888.com" { type master; file "/etc/bind/db.hazard-redirect"; }; # dodano: 2017-05-24T07:46:16
```

(...)

2. Dla Dnsmasq zaś:

```
## 30-05-2017 18:59:21
```

```
145.237.235.240 www.slbet.com # dodano: 2017-05-26T08:53:41
```

```
145.237.235.240 betcris888.com # dodano: 2017-05-24T07:46:16
```

(...)

3. A dla popularnej w małych sieciach platformy Mikrotik tak:

```
## 30-05-2017 18:59:21
```

```
/ip dns static remove [find comment~"# hazard"]
```

```
/ip dns static
```

```
:do { add name="www.slbet.com" address="145.237.235.240" disabled=no comment="# hazard # dodano: 2017-05-26T08:53:41"; } on-error={ set [find name="www.slbet.com"] address="145.237.235.240" disabled=no comment="# hazard # dodano: 2017-05-26T08:53:41"; }
```

```
:do { add name="betcris888.com" address="145.237.235.240" disabled=no comment="# hazard # dodano: 2017-05-24T07:46:16"; } on-error={ set [find name="betcris888.com"] address="145.237.235.240" disabled=no comment="# hazard # dodano: 2017-05-24T07:46:16"; }
```

```
(...)
```

Publikacja gotowych plików dla w/w platform nie stanowi technicznego problemu dla MF, a uprościłaby i upowszechniłaby implementację RDZ nie tylko w sieciach małych operatorów, ale i wśród podmiotów nie objętych dyspozycją ustawy hazardowej. Możliwość pobierania gotowych plików konfiguracyjnych mogłaby bowiem być użyteczna np. dla administratorów sieci korporacyjnych, akademickich, czy samorządowych. Podmioty te z własnych powodów mogą chętnie sięgnąć po proste w użyciu narzędzie do blokowania stron hazardowych, a reguły np. korporacyjnego zarządzania infrastrukturą teleinformatyczną wykluczające możliwość np. dowolnego konfigurowania adresów DNS lub instalowania dodatkowego oprogramowania, mogą pozytywnie wpłynąć na powszechność implementacji RDZ. W ocenie KIKE warto rozważyć więc udostępnianie RDZ równoległe nie tylko w formacie XML, ale i w/w gotowych plików dla najpopularniejszych serwerów DNS/DNS cache.

* * *

Mamy nadzieję, że Pan Minister poleci udzielenie odpowiedzi na wyrażone w niniejszym piśmie wątpliwości, a także rozważenie proponowanych przez nas rozwiązań, takich jak zmiana ustawy lub choćby wydanie wytycznych, które pomogłyby małym operatorom właściwie realizować spoczywające na nich obowiązki.

Z poważaniem,

Piotr Marciniak

Kinga Pawłowska-Nojszewska

Prezes Zarządu KIKE

Radca prawny

Grupa Robocza ds. Administracji Publicznej

Grupa Robocza ds. Administracji Publicznej

KIKE

KIKE

Do wiadomości:

Pani Anna Streżyńska
Minister Cyfryzacji

Pan Marcin Cichy
Prezes Urzędu Komunikacji Elektronicznej

Pan dr inż. Jerzy Żurek
Dyrektor Instytutu Łączności – Państwowego Instytutu Badawczego

Pan Wojciech Kamieniecki
Dyrektor Naukowej i Akademickiej Sieci Komputerowej