Podszywanie się – prawo vs protokoły

Udawanie innej osoby, zwłaszcza w celach szalbierczych, to oszustwo stare jak świat. W klasycznej postaci było i jest związane z konkretnym, realnym człowiekiem. Tyle że w czasach nam współczesnych – wieku techniki, porozumiewania się na odległość, Internetu – pojawiły się rozwiązania skutecznie chroniące owego szalbierza przed identyfikacją.

Jednym z takich rozwiązań jest telekomunikacyjne podszywanie się (ang. *spoofing Caller ID*). *Caller ID*, czyli identyfikację numeru inicjującego połączenie i możliwość prezentowania go na urządzeniu odbierającym, umożliwiały już sieci analogowe. W sieciach cyfrowych (usługa CLIP), w których są bramki VoIP, tę identyfikację można modyfikować (a nawet – nie posiadając jakiegokolwiek realnego numeru telefonu – dowolnie ustalać) i wykonywać połączenia podszywające się pod taką identyfikację. Dodatkowo korzystanie z odpowiedniego oprogramowania syntezującego chroni oszusta przed ujawnieniem jego głosu. Tak więc jedna z cech protokołów cyfrowych, bo przecież nie błąd, ułatwiła oszustwa, przeważnie złośliwe lub właśnie szalbiercze, wyłudzające środki finansowe czy dane. Problem był od dawna znany, przede wszystkim w USA, a od pewnego czasu proceder ten jest tam zakazany.

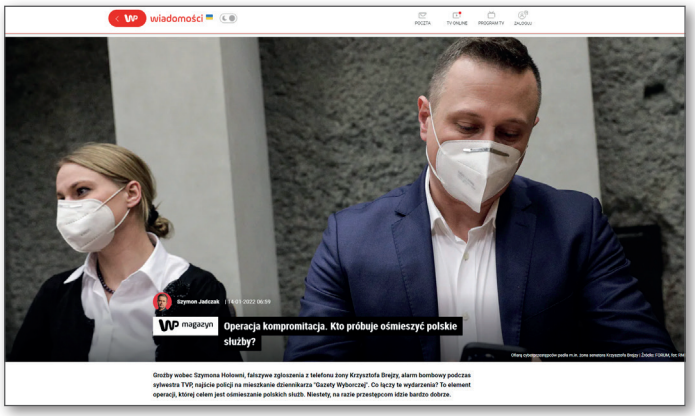
Janusz Dorożyński

adiunkt badawczo-dydaktyczny Instytutu Informatyki Uniwersytetu KazimierzaWielkiego w Bydgoszczy. Absolwent Moskiewskiego Instytutu Subtelnej Technologii Chemicznej im. Łomonosowa (obecnie część Moskiewskiego Uniwersytetu Technologicznego). W 1984 r. na tej uczelni uzyskał stopień doktora nauk technicznych. W pracy zawodowej do 2017 r. związany z przemysłem informatycznym. Członek PTI od 1985 r.

Na naszym podwórku

W Polsce już dwanaście lat temu portal niebezpiecznik.pl (https://niebezpiecznik.pl/post/4-lata-wiezienia-za-spoofing-callerid-dla-polaka/) informował o mechanizmie bramki VoIP modyfikującym prezentację numeru telefonu komórkowego w związku z postępowaniem prokuratorskim i sądowym, zakończonym wyrokiem 4 lat pozbawienia wolności w zawieszeniu. Już wtedy prokuratura zauważyła brak jednoznacznych uregulowań prawnych, nakazujących prezentowanie zgodnej z rzeczywistością informacji o numerze wywołującym połączenie. I nawet miała wystąpić do ówczesnego Ministerstwa Infrastruktury o spowodowanie wprowadzenia stosownych zmian. Tak się jednak nie stało.

Telefoniczne, ale nie tylko, złośliwe podszywanie się pod pracowników banków czy policjantów było dość powszechnym zjawiskiem, a poszkodowani przez taki proceder byli nawet często traktowani jak sprawcy oszustwa (https://wiadomosci.wp.pl/operacja-kompromitacja-kto-probuje-osmieszyc-polskie-sluzby-6726030993075168a).



I być może dopiero przypadki podszywania się pod numery telefonów znanych osób – jak byłego szefa CBA Pawła Wojtunika (z jego telefonu na początku tego roku przekazano córce makabryczną informację o jego śmierci) – doprowadziły do przedstawienia przez rząd 15 czerwca br. projektu ustawy dotyczącej zwalczania nadużyć w komunikacji elektronicznej (https://legislacja.rcl.gov.pl/projekt/12360854).

Zakres ustawy

Ustawa dotyczy szerszego spektrum oszustw – nie tylko telefonicznych, lecz także szalbierczych mejli, esemesów czy witryn www. Wynika to z zaproponowanych kluczowych definicji komunikatu cyfrowego oraz cyfrowego nadużycia. Komunikat cyfrowy oznacza dowolną informację przekazywaną pomiędzy użytkownikami poprzez publiczne usługi telekomunikacyjne lub usługi komunikacji niewykorzystującej numerów (z oczywistym wyłączeniem radiofonii lub telewizji). Za cyfrowe nadużycie uważane jest świadczenie usługi telekomunikacyjnej lub używanie urządzeń telekomunikacyjnych niezgodnie z ich przeznaczeniem lub przepisami prawa, których celem lub skutkiem jest wyrządzenie szkody odbiorcy lub wyłudzenie nienależnych korzyści. Dotyczy to w szczególności zakazu generowania sztucznego ruchu, wysyłania esemesów lub wykonywania połączeń głosowych nakłaniających m.in. do przekazania danych osobowych, niekorzystnego rozporządzenia majątkiem, przekierowania na stronę internetową, kontaktu telefonicznego lub instalacji oprogramowania, a działania takie są zagrożone nawet karą do 5 lat pozbawienia wolności.

Cel proponowanej i dawno oczekiwanej ustawy (już w 2017 r. na witrynie stowarzyszenia ISACA w kontekście kolejnej regulacji w USA pytano: „A kiedy w Polsce?") – jest oczywisty. Daje ona jednoznaczną podstawę prawną do ścigania opisanych wyżej szalbierstw. Omawiany projekt wszedł na standardową ścieżkę legislacyjną, został skierowany do uzgodnień z ministerstwami, zaopiniowania z wybranymi urzędami centralnymi oraz do konsultacji z 58 organizacjami pozarządowymi, z których 13 przedstawiło swoje uwagi organizacji, w tym PTI i PIIT.

Nasza opinia

Stanowisko PTI zwraca uwagę na kilka aspektów. Dwa z nich mają charakter ogólny, pozostałe – specjalistyczny. Ogólnej natury jest kwestia terminologiczna, zobowiązująca ze względu na nazwę i misję naszego stowarzyszenia oraz zwracająca uwagę na zagnieżdżenia się w polskiej terminologii anglicyzmów, a nawet ostatnich zapożyczeń, jak *phishing* czy *spoofing*. Proponujemy użycie w ustawie określenia *esemes* (występującego w słowniku PWN) zamiast angielskiego skrótowca SMS oraz określeń: szalbierczy *esemes* i szalbierczy numer dzwoniącego zamiast *smishing* i *CLI spoofing*. Pojęcie „szalbierstwo" wprawdzie należy do stylu wysokiego, książkowego, ale jest też terminem prawniczym, występuje w kodeksie wykroczeń. Wprowadzenie takiego określenia jednoznacznie wskazywałoby na negatywne skutki odbioru oszukańczego esemesa czy rozmowy z podszywającego się numeru dzwoniącego.

Drugim ogólnym stwierdzeniem jest zwrócenie uwagi na pominięcie w projekcie ustawy innych form komunikacji elektronicznej. W szczególności nie ma wskazania takich form, jak komunikatory (WhatApps, Telegram itp.) oraz media społecznościowe, w tym różnego typu fora ogłoszeniowe, mimo że i w ich przypadku obserwuje się znaczący wzrost nadużywania wysyłania oraz publikowania treści dezinformujących czy mogących doprowadzić do szkodliwych dla odbiorcy działań. Na ten aspekt zwróciły uwagę także inne organizacje i instytucje opiniujące projekt ustawy.

Propozycje PTI

W zakresie specjalistycznym mamy kilka sugestii. Ponieważ w ustawie zawarto definicję poczty elektronicznej odnoszącą się do protokołów SMTP, POP3 i IMAP4, uważamy, że w definicji nie należy umieszczać nazw produktów/protokołów, które mogą się z czasem technicznie zmieniać i występować pod innymi nazwami – wystarczy podać jedynie charakterystyczny protokół SMTP z ogólnym dopuszczeniem protokołów go rozszerzających.

W regulacji określającej sztuczny ruch projekt zaznacza, że jest to związane z wysyłaniem lub odbieraniem komunikatów cyfrowych. Proponujemy usunięcie wskazania odbierania, gdyż odbiorca takich komunikatów elektronicznych nie ma wpływu (oprócz całkowitej blokady dostępu do wszystkich komunikatów) na ich odbieranie. Jedynie po rozpoznaniu, mając odpowiednią wiedzę lub doświadczenie, może je zakończyć lub usunąć. W żadnym stopniu nie może odpowiadać za ich rozpowszechnianie, jeżeli ich dalej nie rozsyła, pod warunkiem że ma wiedzę, że są one komunikatami szalbierskimi.

Projekt przewiduje tworzenie i ogłaszanie przez jednostkę monitorującą CSIRT NASK wzorców szalbierczych esemesów, które będą w komunikacji blokowane, ale bez wskazania podstawy do blokady. Uniemożliwia to skuteczny uzasadniony sprzeciw wobec decyzji CSIRT, ponieważ nie będą jawnie wskazane (nie będą ogłoszone) zarzuty uzasadniające blokadę, a to byłoby to sprzeczne z jedną z zasad prawodawstwa, iż wymagane może być tylko prawo ogłoszone. Wnioskujemy więc o dodanie odpowiednich zapisów.

W szczegółowym przepisie dotyczącym zwalczania telefonicznego podszywania się projekt przewiduje blokowanie połączenia lub ukrywanie identyfikacji numeru inicjującego połączenia. Według opinii PTI ukrywanie identyfikacji będzie przeciwskuteczne, gdyż połączenie będzie odbierane bez świadomości podszywania się. Dlatego sugerujemy, aby w tym przypadku ograniczyć się tylko do blokowania połączenia, z podaniem informacji o tym fakcie oraz o podstawie do zablokowania.

Kolejne przepisy wprowadzają utrzymywanie jawnej listy szalbierczych stron internetowych ze wskazaniem nazwy domenowej tych stron oraz dają prawo dostawcy usług telekomunikacyjnych do ich blokowania. Uważamy, że szkodliwe mogą być tylko niektóre witryny www z danej domeny, więc wskazania powinno się ograniczyć do stron (witryn) internetowych, a nie domen. Natomiast blokowanie powinno mieć uzasadnienie, które dostawca byłby zobowiązany wskazać przy blokowaniu konkretnych stron internetowych. Taka modyfikacja nie spowoduje dezorientacji użytkownika końcowego, gdyż odmowa świadczenia usługi (blokada) będzie umotywowana prawnie, ale nie technicznie, np. w postaci kodów błędów protokołu http.

Ostatnią analizowaną w opinii kwestią specjalistyczną jest przepis, wskazujący aktywne konta poczty elektronicznej i zobowiązujący dostawców takiej poczty dla ponad 500 tysięcy kont/użytkowników stosowanie enumeratywne trzech mechanizmów ochronnych: SPR, DMARC, DKIM. Zwróciliśmy uwagę, że nie nie ma definicji czym jest aktywne konto pocztowe. Wiele zarejestrowanych kont może być latami nieaktywnych, ale użytecznych dla ich właścicieli. Jedynym kryterium dla obsługującego konta jest opłacenie lub spełnianie określonych wymagań. W związku z tym w naszej propozycji zalecamy zastąpienie określenia „aktywne" określeniem „zarejestrowane". Kolejna sprawa – enumeratywne wymuszanie stosowania tylko trzech rozwiązań ochronnych jest ułomne, gdyż istnieją jeszcze inne metody, jak ADSP, VBR, iprev, DNSWL. Dlatego proponujemy, aby dostawcy wyszukiwali i stosowali jeden z wybranych (najlepszych) mechanizmów potwierdzania wiarygodności podanego nadawcy mejla. Zwróciliśmy też uwagę na pominięcie mniejszych dostawców poczty elektronicznej bez uzasadnienia w towarzyszących projektowi dokumentach OSP. Dotyczyło to też granicznej liczby 500 tysięcy kont/użytkowników.

Ustawa jest bardzo potrzebna i powinna zostać wprowadzona bez zwłoki. Niestety, być może ze względu na okres kanikuły, proces legislacyjny zamarł. Ostatnie zmiany na stronie projektu zostały dokonane 7 lipca br. Nie ma informacji o odniesieniu się ministerstwa do zgłoszonych uwag i opinii, nie ma też informacji o przewidzianej konferencji uzgodnieniowej. Niewątpliwe należy śledzić postęp tego procesu.