POLSKIE TOWARZYSTWO INFORMATYCZNE
IZBA RZECZOZNAWCÓW

Izba Rzeczoznawców PTI, ul. Solec 38 lok. 103, 00-394 Warszawa, tel.: +48 22 887 31 47, +48 22 838 47 05, e-mail: ir@pti.org.pl, www.pti.org.pl/ir

Warszawa, dn. 01.07.2022 r.

Kancelaria Prezesa Rady Ministrów

Departament Rozwoju Cyfrowego

Al. Ujazdowskie 1/3

00-583 Warszawa

dot.: ***projekt ustawy o zwalczaniu nadużyć w komunikacji elektronicznej (RD402)***

W odpowiedzi na skierowaną do Polskiego Towarzystwa Informatycznego prośbę o opinię dotyczącą udostępnionego w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny **projektu ustawy o zwalczaniu nadużyć w komunikacji elektronicznej (RD402)** z upoważnienia Prezesa Polskiego Towarzystwa Informatycznego przedstawiam poniżej nasze stanowisko w przedmiotowej sprawie.

Propozycje modyfikacji projektu ustawy

ad Art. 1 pkt 2) zasady wnoszenia sprzeciwu przez nadawcę krótkiej wiadomości tekstowej (SMS), wobec uznania treści takiej wiadomości za wyczerpującą znamiona nadużycia w komunikacji elektronicznej;

Propozycja PTI

Przyjąć, w całym tekście ustawy, dopuszczony przez słownik PWN termin **esemes** (wraz z jego odmianą rzeczownikową) zamiast angielskiego skrótu SMS (patrz „Uwaga ogólna").

ad Art. 2 pkt 8) poczta elektroniczna – usługę komunikacji interpersonalnej niewykorzystującą numerów, która umożliwia przekazywanie komunikatu elektronicznego z wykorzystaniem standardu SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol), lub IMAP4 (Internet Message Access Protocol);

Propozycja PTI

Powyższą definicję skrócić do postaci:

poczta elektroniczna – usługa przekazywania komunikatu elektronicznego z wykorzystaniem protokołu SMTP bądź protokołów będących jego rozszerzeniem.

Komentarz PTI

W treści ustawy 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. Fraza *...komunikacji interpersonalnej niewykorzystującą numerów, …* jest niepotrzebna.

ad Art. 3. ust. 1. pkt 1) inicjowania wysyłania lub odbierania komunikatów elektronicznych lub połączeń głosowych w sieci telekomunikacyjnej z wykorzystaniem urządzeń telekomunikacyjnych lub programów, których celem nie jest skorzystanie z usługi telekomunikacyjnej, lecz ich zarejestrowanie na punkcie połączenia sieci telekomunikacyjnych bądź przez systemy rozliczeniowe (sztuczny ruch);

Propozycja PTI

Usunąć frazę

...lub odbierania….

Komentarz PTI

Wpisanie frazy *...lub odbierania….* nie ma uzasadnienia, 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.

ad Art. 3 ust. 1. pkt 2) wysyłania krótkich wiadomości tekstowych (SMS), w których nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem, przekierowania na stronę internetową, żądania kontaktu telefonicznego lub instalacji oprogramowania (smishing);

Propozycja PTI

W danym przepisie i w całym tekście ustawy używanie terminu **esemes** (zamiast SMS) oraz nazwanie tych komunikatów terminem **esemesy szalbierskie**.

Komentarz PTI

Rozwinięcie jest zawarte w uwadze ogólnej.

ad Art. 3 ust. 1 pkt 3) nieuprawnionego posłużenia się przez użytkownika wywołującego połączenie głosowe informacją adresową wskazującą na osobę lub jednostkę organizacyjną inną niż ten użytkownik, służące podszyciu się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji oprogramowania (CLI spoofing).

Propozycja PTI

Wprowadzenie zamiast określenia „(CLI spoofing)" terminu:

szalbierczy numer dzwoniącego

Komentarz PTI

Termin CLI spoofing jest mało zrozumiały. Już lepszy byłby termin Caller ID spoofing, gdyby nie był angielski, dlatego proponujemy używanie terminu - **szalbierczy numer dzwoniącego,** jednoznacznie wskazujący na szkodliwy identyfikator dzwoniącego.

ad Art. 4. ust. 2. CSIRT NASK na podstawie monitorowania, o którym mowa w ust. 1, tworzy wzorzec wiadomości wyczerpującej znamiona smishingu.

Propozycja PTI

W powyższym przepisie na jego końcu, zamiast słowa ...smishingu… :

szalbierskiego esemsesa wraz z podaniem zarzutów go dotyczących.

Komentarz PTI

Uważamy, iż przy każdym zablokowanym rodzaju esemesa powinny być wpisane zarzuty jego dotyczące, będące podstawą blokady. Proponowania zmiana jest związana z kolejnym przepisem z art. 5, gdyż umożliwia skuteczny sprzeciw wobec decyzji CSIRT definiującej znamiona ~~-~~szalbierskiego esemesa (*smishingu*).

ad Art. 5. ust. 1. Nadawca krótkiej wiadomości tekstowej (SMS) może wnieść do Prezesa UKE sprzeciw wobec uznania treści takiej wiadomości za wyczerpującą znamiona smishingu.

ust. 2. Sprzeciw zawiera: 1) uzasadnienie wyjaśniające dlaczego treść krótkiej wiadomości tekstowej (SMS) nie wyczerpuje znamion smishingu;

Komentarz PTI

W przypadku zaakceptowania propozycji PTI powyżej do art. 4 ust. 2 powyższy przepis nie budzi wątpliwości. Jednakże pozostawienie takiej treści art. 5.1 i 2 bez proponowanej zmiany PTI w art. 4 ust. 2 spowoduje, iż nie będzie możliwe skuteczne sprzeciwienie się zarzutowi szalbierstwa w esemesie (smishingu), ponieważ nie będą jawne wskazane (nie będą ogłoszone) zarzuty uzasadniające blokadę. Byłoby to sprzeczne z jedną spośród zasad prawodawstwa, iż wymagane może być tylko prawo ogłoszone.

ad Art. 8. W celu zapobiegania i zwalczania CLI spoofing przedsiębiorca telekomunikacyjny blokuje połączenie głosowe albo *ukrywa identyfikację numeru wywołującego* dla użytkownika końcowego.

Propozycja PTI

Zamienić cały powyższy przepis na poniższy:

W celu zapobiegania i zwalczania odbioru połączeń z szalbierczych numerów dzwoniących przedsiębiorca telekomunikacyjny blokuje połączenie głosowe i podaje informację o zablokowaniu połączenia i jego przyczynie.

Komentarz PTI

Ukrycie identyfikacji szalbierczego numeru wywołującego nie tylko nie wystarczy, ale doprowadzi do skutku przeciwnego niż zamierzony przez regulację – połączenie będzie odbierane bez świadomości szalbierstwa.

ad Art. 11. ust. 1. W celu ochrony użytkowników internetu przed stronami internetowymi wyłudzającymi dane, w tym dane osobowe oraz doprowadzającymi użytkowników internetu do niekorzystnego rozporządzenia ich majątkiem, może zostać zawarte porozumienie w zakresie prowadzenia i utrzymywania jawnej listy ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników internetu oraz uniemożliwienia dostępu do tych stron.

Propozycja PTI zmiany treści zapisu:

W celu ochrony użytkowników internetu przed szalbierczymi stronami internetowymi wyłudzającymi dane, w tym dane osobowe oraz doprowadzającymi użytkowników internetu do niekorzystnego rozporządzenia ich majątkiem, może zostać zawarte porozumienie w zakresie prowadzenia i utrzymywania jawnej listy ostrzeżeń dotyczących szalbierczych stron internetowych oraz uniemożliwienia do nich dostępu.

Komentarz PTI

Takimi szalbierczymi stronami mogą być tylko niektóre strony z danej domeny. Wobec tego blokowanie całej domeny jest działaniem nadmiarowym – należy się ograniczyć tylko do blokowania stron.

ad Art. 11. ust.2. W celu ochrony użytkowników internetu przed CLI spoofing, elementem porozumienia, o którym mowa w ust. 1, może być jawna lista ostrzeżeń dotyczących domen internetowych, które służą do nieuprawnionego wykorzystania numeru lub identyfikatora użytkownika wywołującego połączenie głosowe oraz uniemożliwienia dostępu do tych stron.

Komentarz PTI

Ten ustęp jest zbędny, gdyż CLI spoofing dotyczy połączeń głosowych a nie stron internetowych, chyba że chodzi tutaj o strony internetowe, które służą podmianie lub ukryciu prawdziwego numeru dzwoniącego. W tym przypadku można je po prostu uznać za strony szalbiercze i potraktować jak te z ust.1. Ale też przy istnieniu VPN uniemożliwianie dostępu do tych stron może być mało skuteczne.

ad Art. 11 ust 3. , 4., 5., 6.

Propozycja PTI zmiany treści zapisu:

W tych ustępach należy wpisać strony internetowe, a nie domeny internetowe.

ad Art. ust.5 Porozumienie określa co najmniej zasady współpracy między stronami, w tym zasady zgłaszania domen internetowych, wpisania oraz usuwania ich z listy ostrzeżeń, o której mowa w ust. 1.

Propozycja PTI zmiany treści zapisu – należy go zmodyfikować jak poniżej:

Porozumienie określa co najmniej zasady współpracy między stronami, w tym zasady i podstawy zgłaszania, wpisania, blokowania oraz zwalniania stron internetowych z listy ostrzeżeń, o której mowa w ust. 1.

Komentarz PTI

Uważamy, iż przyczyny powodujące zgłoszenie muszą być jawne, gdyż łączne z proponowaną zmianą w ust. 6 art. 11 nie spowoduje to dezorientacji użytkownika w sytuacji odmowy świadczenia usługi dostępu do konkretnej strony. Ponadto proponowane uzupełnienie zapobiegnie arbitralnemu blokowaniu dostępu do stron internetowych.

ad Art. 11 ust. 6. Przedsiębiorca telekomunikacyjny może uniemożliwić użytkownikom internetu dostęp do stron internetowych wpisanych na listę, o której mowa w ust. 1.

Propozycja PTI

Należy dodać przed końcową kropką poniższy fragment:

, wraz z podaniem przyczyny blokady.

Komentarz PTI

W związku w danym przepisem w przypadku zaakceptowania propozycji PTI powyżej do art. 11 ust. 1 powyższy przepis nie spowoduje dezorientacji użytkownika końcowego, gdyż odmowa świadczenia usługi (blokada) będzie umotywowana prawnie, ale nie technicznie, np. w postaci kodów błędów protokołu http.

ad Art. 12. ust. 1. Dostawca poczty elektronicznej:

1) dla co najmniej 500 000 użytkowników,
2) dla podmiotu publicznego, lub
3) obsługujący co najmniej 500 000 aktywnych kont pocztowych

– ma obowiązek stosowania mechanizmu SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication Reporting and Conformance) oraz DKIM (DomainKeys Identified Mail).

Propozycja PTI

Zmodyfikować zapis powyższego ustępu na poniższy (opis modyfikacji w komentarzu):

Dostawca poczty elektronicznej:

1) dla co najmniej 500 000 użytkowników,
2) dla podmiotu publicznego, lub
3) obsługujący co najmniej 500 000 zarejestrowanych kont pocztowych

– jest zobowiązany do wyboru i do stosowania jednego lub wielu ze znanych mechanizmów potwierdzania wiarygodności podanego nadawcy mejla, w szczególności takich jak SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication Reporting and Conformance), DKIM (DomainKeys Identified Mail).

Komentarz PTI

Nie jest znana definicja, czym jest aktywne konto pocztowe. Wiele zarejestrowanych kont może być latami nieaktywnych, ale być dla ich właściciela użytecznymi. Jedynym kryterium dla obsługującego konta jest opłacenie lub spełnianie określonych wymagań. W związku z tym w propozycji zastąpiono określenie „aktywnych" na określenie „zarejestrowanych".

W propozycji PTI nie ma wymuszania stosowania wymienionych mechanizmów (wszystkich lub jednego z nich, jak SPF, DMARC, DKIM), gdyż istnieją jeszcze inne metody (ADSP, VBR, iprev, DNSWL). W związku z tym modyfikacja ogranicza się do tego, iż dostawcy mają wyszukiwać i stosować jeden z wybranych (najlepszych) mechanizmów potwierdzania wiarygodności prawdziwości podanego nadawcy mejla.

Natomiast obie redakcje budzą trzy wątpliwości.

Po pierwsze dlaczego pomija się mniejszych dostawców usług poczty elektronicznej oraz dostawców zagranicznych, często szczególnie nadużywających, nawet w celach przestępczych komunikacji elektronicznej. Wydaje się, że konieczne jest określenie możliwych do realizacji sankcji wobec takich przypadków.

Po drugie nie jest jasna intencja twórców propozycji jakie warunki 1), 2), 3) ma spełnić dostawca – czy łącznie 1) i 2) lub 3), czy dowolny z tych trzech? Jeśli łącznie 1) i 2), to bardziej klarownym byłoby połączenie 1) i 2). Aczkolwiek to by wyłączyło obsługę podmiotów publicznych z mniej niż 500 tys. użytkowników, co jest z pewnością wbrew intencjom autorów propozycji, gdyż prawdopodobnie w skali kraju może nie być ani jednego podmiotu publicznego z taką liczbą użytkowników. Proponujemy więc z wyliczenia usunąć spójnik „lub", a przed dwukropkiem dodać „spełniający co najmniej jeden z poniższych warunków".

Po trzecie brak jest uzasadnienia dla liczby 500 tysięcy użytkowników/kont. Powinno się ono znaleźć co najmniej w dokumencie OSR.

Komentarz ogólny

W odniesieniu do całej treści ustawy i w szczególności do art. 1 – projektowana regulacja nie odnosi się do innych niż ujęte w propozycji formy komunikacji elektronicznej takie jak komunikatory oraz media społecznościowe, gdzie szczególnie ostatnio silnie rośnie nadużywanie wysyłania oraz publikowania treści dezinformujących oraz wymuszających szkodliwe dla odbiorcy działania. W obecnej postaci ustawa tylko częściowo będzie spełniać rolę zwalczania nadużyć w komunikacji elektronicznej.

Uwaga ogólna

W USTAWIE z dnia 7 października 1999 r. o języku polskim (Dz. U. z 2021 r. poz. 672) w **Art. 4. Język polski jest językiem urzędowym: 1) konstytucyjnych organów państwa;** oraz w **Art. 5. 1. Podmioty wykonujące zadania publiczne na terytorium Rzeczypospolitej Polskiej dokonują wszelkich czynności urzędowych oraz składają oświadczenia woli w języku polskim, chyba że przepisy szczególne stanowią inaczej.** Oznacza to, że również teksty uchwalanych ustaw powinny być w języku polskim, z zastrzeżeniem **Art. 11. Przepisy art. 5–10 nie dotyczą: 5) zwyczajowo stosowanej terminologii naukowej i technicznej;**

Powyższe zastrzeżenie może być skuteczne jedynie, gdy konieczne do wskazania w treści terminy nie mają odpowiedników w języku polskim.

W przypadku treści projektu ustawy (RD402) proponujemy na terminy:

- SMS – krótka wiadomość tekstowa, która w języku polskim, zamiast skrótu SMS, może być opisana terminem **esemes** wraz z możliwością jego odmiany (taki termin występuje w słowniku PWN),
- smishing – szalbierczy esemes
- CLI spoofing – szalbierczy numer dzwoniącego

Proponując wprowadzenie terminu **szalbierczy** jednoznacznie wskazujemy na negatywny odbiór takiego esemesa oraz rozmowy z podszywającego się numeru dzwoniącego. Termin ten można też używać przypadku phishingu – szalbierczej strony oraz szalbierczego mejla. Tekst tej ustawy może przy tej okazji również wprowadzić polską jednoznacznie zrozumiałą terminologię ostrzegania przed nadużyciami w komunikacji elektronicznej.

Opracował zespół:

Wacław Iszkowski, Witold Rakoczy, Andrzej Szczerba;

współpraca i redakcja: Janusz Dorożyński.

Tomasz Szatkowski

Dyrektor Izby Rzeczoznawców

Polskie Towarzystwo Informatyczne