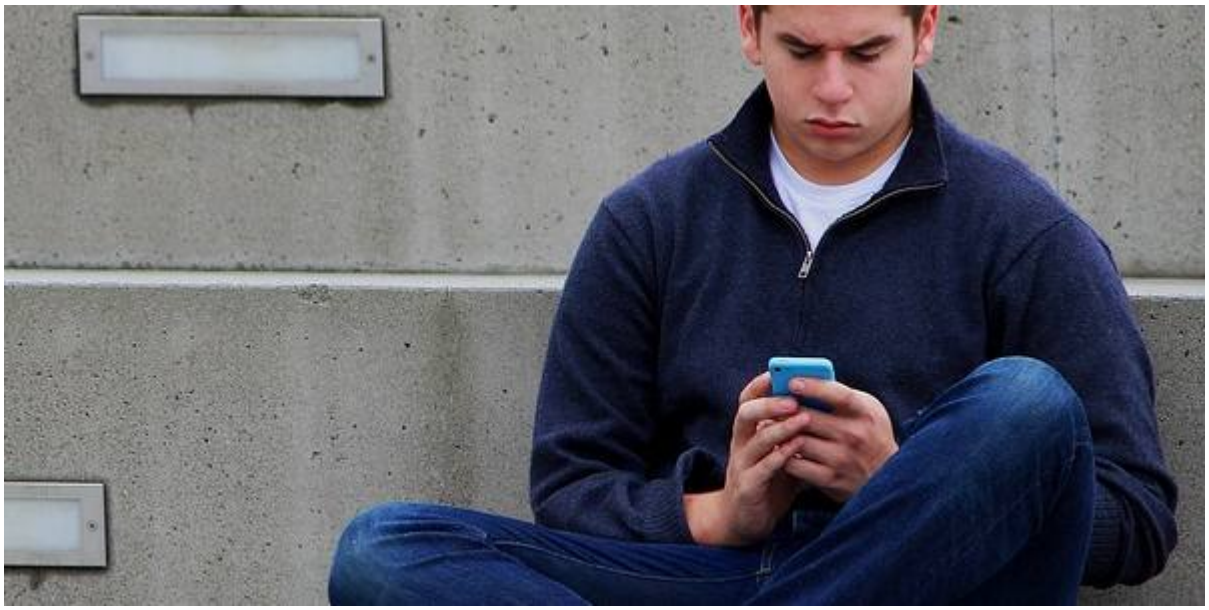
Chcą rozprawić się z fałszywymi SMS-ami i wyłudzeniami

2 sierpnia 2022

Usługi telekomunikacyjne są coraz częściej i w coraz bardziej wyszukany sposób wykorzystywane przez cyberprzestępców do oszustw i wyłudzeń. Dotychczasowe przepisy w niewystarczający sposób regulują tę kwestię, dlatego w KPRM przygotowano projekt ustawy o zwalczaniu nadużyć w komunikacji elektronicznej, który jest w tej chwili na etapie opiniowania. Przewiduje on m.in. wprowadzenie wzorca wiadomości SMS o charakterze smishingowym i stworzenie listy domen internetowych, które służą wyłącznie do wyłudzeń danych i środków finansowych. Na dostawców poczty elektronicznej i firmy telekomunikacyjne zostaną też nałożone nowe obowiązki w zakresie bezpieczeństwa, za których niedopełnienie grozić będą kary.



„Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej to jest akt prawny, który ma wykorzystać dostępną już dzisiaj technologię do tego, aby zwalczać przestępczość, która w ostatnich miesiącach i latach stała się szczególnie dotkliwa

dla obywateli i przedsiębiorców. Chodzi przede wszystkim o podszywanie się pod kogoś i doprowadzenie do tego, aby oddał dostęp do swoich zasobów albo rozporządzał pieniędzmi w sposób niezgodny ze swoim interesem" – mówi agencji Newseria Biznes Janusz Cieszyński, sekretarz stanu w KPRM i rządowy pełnomocnik ds. cyberbezpieczeństwa.

Projekt ustawy o zwalczaniu nadużyć w komunikacji elektronicznej został opublikowany 15 czerwca br. na stronie Rządowego Centrum Legislacji. Przeszedł już uzgodnienia międzyresortowe i konsultacje publiczne, a w tej chwili jest na etapie opiniowania. Celem nowej regulacji ma być ograniczenie skali nadużyć i zapewnienie bezpieczeństwa użytkownikom w dobie nasilających się ataków wykorzystujących usługi telekomunikacyjne.

Projekt skupia się przede wszystkim na przeciwdziałaniu tzw. spoofingowi, czyli wyłudzaniu danych (np. informacji o karcie kredytowej) albo infekowaniu telefonu za pomocą odpowiednio spreparowanej wiadomości SMS, oraz eliminacji przypadków tzw. Caller ID spoofingu, czyli zmiany identyfikatora rozmówcy na zaufany albo rozpoznawalny dla adresata w celu nakłonienia go do określonego zachowania. „Chcemy takim zjawiskom przeciwdziałać, ponieważ ich skala i szkodliwość społeczna stale rośnie" – podkreśla Janusz Cieszyński. „Dlatego wspólnie z rynkiem, przedsiębiorcami z branży telekomunikacyjnej wypracowaliśmy rozwiązania, które, po pierwsze, uniemożliwią wykonanie połączeń telefonicznych, które podają się za połączenie z numeru innego niż faktyczny. Druga kwestia to ograniczenie możliwości rozsyłania na masową skalę SMS-ów phishingowych zawierających złośliwą treść. Chcemy, żeby takie wzorce niebezpiecznych wiadomości były wspólnie przetwarzane przez operatorów telekomunikacyjnych i w momencie wykrycia u choćby jednego były wyłączane dla całej populacji i dla wszystkich przedsiębiorców".

Zgodnie z projektem na przedsiębiorców telekomunikacyjnych zostanie nałożony obowiązek blokowania SMS-ów zawierających

treści zgodne ze wzorcem wiadomości przekazanym przez CSIRT NASK. Jego zadaniem będzie z kolei uruchomienie (w terminie trzech miesięcy od wejścia w życie nowej ustawy) systemu teleinformatycznego przekazującego wzorce takich wiadomości. Do tego systemu podłączeni będą nie tylko operatorzy, ale również Komendant Główny Policji i Prezes Urzędu Komunikacji Elektronicznej. „Kolejną kwestią jest też dodatkowe zabezpieczenie dla poczty elektronicznej, tzn. wprowadzenie protokołów bezpieczeństwa, które sprawią, że wiarygodność nadawcy będzie znacznie wyższa niż do tej pory i uniemożliwi podszycie się pod kogoś innego" – wyjaśnia sekretarz stanu w KPRM.

Nowa ustawa nałoży też dodatkowe obowiązki na dostawców poczty elektronicznej (dla co najmniej 500 tys. użytkowników). Będą oni zobowiązani do zapewnienia mechanizmu uwierzytelnienia poczty.

Co ważne, regulacja wprowadzi też definicję pojęcia „nadużycia w komunikacji elektronicznej". Za takie nadużycie ma być uważane świadczenie usługi telekomunikacyjnej lub korzystanie z urządzeń telekomunikacyjnych niezgodnie z ich przeznaczeniem lub przepisami prawa, którego celem lub skutkiem jest wyrządzenie szkody przedsiębiorcy komunikacyjnemu bądź użytkownikowi końcowemu lub osiągnięcie nienależnych korzyści.

Jak wyjaśnia CERT Polska w raporcie „Krajobraz bezpieczeństwa polskiego internetu 2021", Caller ID spoofing jest możliwy dzięki specjalnym bramkom internetowym VoIP, z których można wykonywać połączenia z wykorzystaniem dowolnego numeru telefonu. Bramki te wykorzystują słabości protokołów używanych w sieciach komórkowych, co oznacza, że operatorzy sieci komórkowych często nie są w stanie zweryfikować, czy połączenie, w ramach którego jest prezentowany numer, faktycznie pochodzi z karty SIM, która jest zarejestrowana dla danego numeru. Caller ID spoofing jest techniką powszechnie używaną również w atakach phishingowych, gdzie przestępcy podszywają się pod bank lub lokalny komisariat policji.

Podobny spoofing można zastosować również w przypadku wiadomości SMS, by podstawić dowolny numer lub nazwę w polu nadawcy. W ubiegłym roku zespół CERT Polska, działający w ramach NASK, odnotował prawie 200-proc. wzrost incydentów phishingowych. Stanowiły one 75 proc. spośród prawie 30 tys. unikalnych incydentów bezpieczeństwa, które zarejestrował CERT Polska w 2021 roku. „Jeżeli chodzi o kary, które przewiduje ten projekt, to są to z jednej strony kary dla osób, które dopuszczają się takich przestępstw, i one wynoszą od trzech miesięcy do pięciu lat pozbawienia wolności. To wydaje się adekwatne, jeżeli popatrzymy na inne czyny zabronione w Kodeksie karnym" – mówi minister Janusz Cieszyński. „Natomiast jeżeli chodzi o kary dla przedsiębiorców, one są podobne jak w innych przypadkach i uzależnione od przychodu, to jest do 3 proc. rocznego obrotu".

Fakultatywne kary administracyjne – nakładane w drodze decyzji przez Prezesa UKE – będą grozić tym podmiotom (przedsiębiorcom telekomunikacyjnym i dostawcom poczty elektronicznej), które nie wywiążą się należycie z nowych obowiązków w zakresie przeciwdziałania nadużyciom w komunikacji elektronicznej. „Trzeba jednak pamiętać o tym, że wysokość tych kar, jeżeli sobie to wyliczymy, patrząc na największych graczy, to nigdy w historii nie była nałożona na takim poziomie, jeżeli chodzi o inne organy, takie jak np. Urząd Komunikacji Elektronicznej. Więc myślę, że chodzi przede wszystkim o to, żeby wskazać, że podmioty świadczące usługi telekomunikacyjne muszą po prostu na poważnie brać te kwestie bezpieczeństwa, ponieważ w przeciwnym razie te kary mogą być dla nich naprawdę dotkliwe" – mówi sekretarz stanu w KPRM.

Autorzy projektu zwracają uwagę, że nowa regulacja jest potrzebna, ponieważ ani Europejski Kodeks Łączności Elektronicznej, ani ustawa Prawo telekomunikacyjne nie zapewniają odpowiednich ram prawnych w celu przeciwdziałania nadużyciom w telekomunikacji elektronicznej, które ostatnimi czasy są coraz bardziej powszechne. Świadczy o tym m.in. fakt,

że środki zapobiegające takim nadużyciom przedsięwzięły już między innymi Wielka Brytania (prowadzenie listy numerów, z których nie są inicjowane połączenia) i Stany Zjednoczone (stosowanie narzędzi umożliwiających uwierzytelnienie informacji adresowej połączenia).

Zdjęcie: Fangirl (CC0)
Źródło: Newseria.pl