Warszawa, 12 lipca 2024 r.

PREZES
URZĘDU KOMUNIKACJI ELEKTRONICZNEJ

REKOMENDACJE

dotyczące środków organizacyjnych i technicznych służących monitorowaniu, wykrywaniu oraz wymianie informacji o CLI spoofing a także blokowaniu połączenia głosowego albo ukrywaniu identyfikacji numeru wywołującego dla użytkownika końcowego

ZATWIERDZAM

Prezes

Jacek Oko

Spis treści

Podstawa prawna

Art. 19 ust. 6 ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. 1703), zwanej dalej „Ustawą" lub „UZNKE".

Wprowadzenie

Ustawa definiuje CLI spoofing (Caller ID spoofing) jako nadużycie polegające na nieuprawnionym posłużeniu się lub korzystaniu przez użytkownika lub przedsiębiorcę telekomunikacyjnego rozpoczynającego połączenie głosowe informacją adresową wskazującą na osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej inną niż ten użytkownik lub przedsiębiorca telekomunikacyjny, służącą podszyciu się pod inny podmiot, w szczególności w celu wywołania strachu, poczucia zagrożenia lub nakłonienia odbiorcy tego połączenia do określonego zachowania, zwłaszcza do przekazania danych osobowych, niekorzystnego rozporządzenia mieniem lub instalacji oprogramowania.

CLI spoofing jest stosowany zarówno przez pojedyncze osoby jak i zorganizowane grupy przestępcze. Celem takiego ataku mogą być osoby prywatne, instytucje, przedsiębiorstwa oraz organizacje. Jest to szczególne zagrożenie dla użytkowników systemów telekomunikacyjnych na całym świecie, zwłaszcza że ataki wykorzystujące CLI spoofing stają się coraz bardziej wyrafinowane i obejmują nowe obszary usług oferowanych przez przedsiębiorstwa telekomunikacyjne i dostawców usług. Istnieje również ryzyko związane z połączeniem CLI spoofing z technologią sztucznej inteligencji, w tym z technologią deepfake.

Możliwość zaistnienia CLI spoofing wynika ze złożoności światowego systemu telekomunikacyjnego, gdzie operatorzy budują i eksploatują swoje sieci zgodnie ze standardami i normami zarządzanymi na poziomie organizacji globalnych, takich jak ITU[1)], 3GPP[2)], ETSI[3)]. Niniejsze standardy nie obejmują jednak rozwiązań bezpieczeństwa, które skutecznie chroniłyby system telekomunikacyjny przed CLI spoofing. Główną przyczyną tego typu oszustw jest niedoskonałość protokołów transmisyjnych, w szczególności możliwość swobodnej zamiany standardów SS7[4)] i SIP[5)] oraz niezależność podmiotów odpowiedzialnych za transfer tych połączeń i ich wprowadzanie do międzynarodowego systemu telekomunikacyjnego.

Dlatego też istotne jest, aby przedsiębiorcy telekomunikacyjni współpracowali ze sobą w celu zwalczania CLI spoofing. Aby to osiągnąć, konieczne jest wprowadzenie jednolitych rozwiązań organizacyjnych i technicznych na poziomie krajowym.

Przeciwdziałanie CLI spoofing powinno obejmować:

1) zapewnienie spójności danych dotyczących wykorzystywanej numeracji;
2) identyfikację możliwych wektorów ataku;
3) monitorowanie zdarzeń wpływających na poziom odporności systemu telekomunikacyjnego;
4) eliminację połączeń zidentyfikowanych jako CLI spoofing.

Powyższe działania mają na celu zwiększenie odporności systemu telekomunikacyjnego w Polsce i jak największe ograniczenie negatywnego wpływu na międzynarodowy system telekomunikacyjny. Niniejsze rekomendacje określają szczegółowe środki organizacyjne i techniczne służące

[1)] International Telecommunication Union.
[2)] 3rd Generation Partnership Project.
[3)] European Telecommunications Standards Institute.
[4)] *Sig*naling System 7.
[5)] Session Initiation Protocol.

monitorowaniu, wykrywaniu oraz wymianie informacji na temat CLI spoofing, a także blokowaniu połączeń głosowych lub ukrywaniu identyfikacji numeru wywołującego dla użytkownika końcowego. Przedmiotowe rekomendacje skierowane są do przedsiębiorców telekomunikacyjnych, którzy nie zawarli porozumienia określającego szczegółowe środki służące monitorowaniu, wykrywaniu oraz wymianie informacji na temat CLI spoofing oraz blokowaniu połączeń głosowych lub ukrywaniu identyfikacji numeru wywołującego dla użytkownika końcowego, o których mowa w art. 19 ust. 2 Ustawy.

Rekomendacje podzielono na cztery bloki tematyczne:

1) Blok A zawierający wskazania dotyczące inicjowania połączeń głosowych;
2) Blok B zawierający wskazania dotyczące możliwości usuwania prezentacji numeru na urządzeniu użytkownika końcowego dla połączeń głosowych;
3) Blok C zawierający wskazania dotyczące możliwości blokowania połączeń głosowych;
4) Blok D zawierający postanowienia dodatkowe zapewniające zdolności do monitorowania podjętych działań w zakresie przeciwdziałania CLI spoofing.

Definicje

1. Abonent – abonent w rozumieniu art. 2 pkt 1 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2024 poz. 34, 731 i 834 z późn. zm.), zwanej dalej „PT".
2. CLI spoofing – definicja w rozumieniu art. 3 ust. 1 pkt 3 UZNKE.
3. Łącze międzynarodowe – infrastruktura techniczna wykorzystywana do zestawienia punktu styku sieci[6)] na potrzeby realizacji połączeń głosowych:
   1) w postaci łącza telekomunikacyjnego, którego chociażby jedno z zakończeń zlokalizowane jest poza granicami Rzeczypospolitej Polskiej lub
   2) łącząca bezpośrednio (tj. bez udziału operatora realizującego tranzyt połączeń) sieć z siecią operatora, który nie jest wpisany do RPT[7] albo którego główna część telekomunikacyjnej infrastruktury dostępowej lub rdzeniowej znajduje się poza granicami Rzeczypospolitej Polskiej i który zgodnie z umową z przedsiębiorcą telekomunikacyjnym wykorzystuje ten punkt styku do przesyłania połączeń międzynarodowych (tj. zainicjowanych poza granicami Rzeczpospolitej Polskiej nie wykorzystujących numeracji z Planu Numeracji Krajowej i zakańczanych na numerze z Planu Numeracji Krajowej).
4. Numer krajowy – zgodnie z §2 ust. 1 pkt 7 Planu numeracji krajowej dla publicznych sieci telefonicznych, w których świadczone są publicznie dostępne usługi telefoniczne[8)] jest to kombinacja cyfr identyfikująca zakończenie sieci, zawierająca WSN (wskaźnik strefy numeracyjnej) lub WST (wyróżnik sieci) oraz pozostałe cyfry numeru zakończenia sieci.
5. Przedsiębiorca telekomunikacyjny – przedsiębiorca telekomunikacyjny w rozumieniu art. 2 pkt 27 PT.
6. Rozwiązanie organizacyjne i techniczne – spełnienie wszystkich wymagań w zakresie realizacji działań związanych ze stosowaniem środków organizacyjnych i technicznych.
7. Użytkownik – użytkownik w rozumieniu art. 2 pkt 49 PT.
8. Użytkownik końcowy – użytkownik końcowy w rozumieniu art. 2 pkt 50 PT.

[6)] Punkt Styku Sieci (PSS) - miejsce połączenia sieci operatora do sieci innego operatora, w którym następuje wymiana ruchu telekomunikacyjnego i sygnalizacji międzysieciowej pomiędzy stronami.
[7)] Rejestr Przedsiębiorców Telekomunikacyjnych.
[8)] „Plan numeracji krajowej dla publicznych sieci telekomunikacyjnych, w których świadczone są publicznie dostępne usługi telefoniczne" stanowi załącznik do Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 30 października 2013 r. w sprawie planu numeracji krajowej dla publicznych sieci telekomunikacyjnych, w których świadczone są publicznie dostępne usługi telefoniczne (Dz. U. z 2023 poz. 145).

Rekomendacje

A.1. Inicjowanie połączenia głosowego.

1. Przedsiębiorca telekomunikacyjny:
   1) jest obowiązany do zapewnienia, że połączenia głosowe inicjowane w jego sieci nie mają znamion CLI spoofing;
   2) zapewnia poprawność i wiarygodność numeru inicjującego połączenie głosowe realizowane przez jego użytkownika końcowego;
   3) zapewnia, że użytkownik końcowy może zainicjować połącznie głosowe wyłącznie z numeru, który został przydzielony abonentowi w umowie o świadczenie usług telekomunikacyjnych zawartej z tym dostawcą, w szczególności numerów krajowych:
      a) przydzielonych w drodze decyzji Prezesa Urzędu Komunikacji Elektronicznej[9)] przedsiębiorcy telekomunikacyjnemu,
      b) udostępnionych lub przeniesionych od innego przedsiębiorcy telekomunikacyjnego[10)].
2. Połączenia inicjowane pomiędzy użytkownikami tego samego przedsiębiorcy telekomunikacyjnego wewnątrz sieci przedsiębiorcy telekomunikacyjnego traktuje się jako zaufane.

A.2. Inicjowanie połączenia głosowego wykorzystującego numerację krajową przez użytkownika końcowego przebywającego za granicą.

1. Połączenie głosowe na numer krajowy nie może być inicjowane poza granicami Polski z wyjątkiem poniższych sytuacji:
   1) jeżeli abonent znajduje się poza terytorium RP i korzysta z abonamentu na usługi telefonii komórkowej przy wykorzystaniu numeru krajowego i łączy się z siecią innego operatora (tzw. roaming) lub
   2) w przypadku, gdy ruch może zostać przeniesiony do Polski w sposób, który oznacza, że połączenie głosowe nie przychodzi do Polski za pośrednictwem łączy międzynarodowych.

[9)] Zgodnie z „Tablicami Zagospodarowania Numeracją" prowadzonymi przez Urząd Komunikacji Elektronicznej: https://numeracja.uke.gov.pl/.

[10)] Zgodnie z danymi dostępnymi poprzez Platformę Lokalizacyjno-Informacyjną z Centralną Bazą Danych (PLI CBD) prowadzoną przez Urząd Komunikacji Elektronicznej.

B.1. Ukrywanie identyfikacji numeru połączeń głosowych dla numeracji krajowej w ruchu krajowym.

1. Zaleca się, aby przedsiębiorca telekomunikacyjny ukrywał identyfikację numeru[11)] połączeń głosowych w ruchu krajowym, gdy zachodzi podejrzenie CLI spoofing, w przypadku braku zgodności z bazą numerów przeniesionych, bazą numerów udostępnionych[12)] i Tablicami Zagospodarowania Numeracji[13)].

B.2. Ukrywanie identyfikacji numeru dla połączeń głosowych prezentujących się numerami krajowymi kierowanych do kraju przez łącza międzynarodowe.

1. Zaleca się, aby przedsiębiorca telekomunikacyjny ukrywał identyfikację numeru dla połączeń głosowych prezentujących się numerami krajowymi stacjonarnymi, kierowanych do kraju poprzez łącza międzynarodowe.

[11)] W przypadku protokołu:
SIP – modyfikacja nagłówka pole priv-value lub Privacy ustawiamy (Privacy: id, user)
ISUP – Address Presentation Restricted Indicator (APRI) ustawiamy „presentation restricted".
[12)] Zgodnie z danymi dostępnymi poprzez Platformę Lokalizacyjno-Informacyjną z Centralną Bazą Danych (PLI CBD) prowadzoną przez Urząd Komunikacji Elektronicznej.
[13)] Zgodnie z „Tablicami Zagospodarowania Numeracją" prowadzonymi przez Urząd Komunikacji Elektronicznej: https://numeracja.uke.gov.pl/.

C.1. Blokowanie[14)] połączeń głosowych przychodzących z numerów krajowych

1. Zaleca się, aby przedsiębiorca telekomunikacyjny blokował przychodzące połączenia głosowe w przypadku, gdy numerem wywołującym połączenie jest:
   1) numer zaczynający się od cyfr AB = 70, 80, 19, 20;
   2) numer alarmowy 99X i 98X;
   3) numer HESC (HESC to zharmonizowany europejski numer skrócony o formacie 11x, gdzie x – jedna, dwie, trzy lub cztery cyfry (w tym m.in. 112, oraz inne: 118 xxx, 116 xxx));
   4) numer dostępu do radiowych sieci przywoławczych (AB=64);
   5) numer przychodzący nie jest zgodny z obowiązującym rozporządzeniem w sprawie planu numeracji krajowej dla publicznych sieci telekomunikacyjnych.
2. Przedsiębiorca telekomunikacyjny blokuje numery znajdujące się na wykazie numerów służących wyłącznie do odbierania połączeń głosowych[15)].

[14)] W przypadku blokady połączenia należy w komunikacji zwrotnej przesłać następujące kody:
- dla SIP – 403 Forbidden,
- dla ISUP – 21 call rejected.

[15)] Prowadzonego przez Prezesa UKE zgodnie z art. 17 ust. 1 UZNKE. Wykaz prowadzony jest pod adresem: https://numeracja.uke.gov.pl/pl/orvc_tables.

D.1. Zgłaszanie nadużyć

1. Przedsiębiorca telekomunikacyjny wykrywając zdarzenie mające znamiona CLI spoofing może zgłosić informację o tym zdarzeniu do Urzędu Komunikacji Elektronicznej na adres skrzynki kontaktowej: cli.uke@uke.gov.pl.
2. Tytuł przekazanej informacji ma następujący format: „CLI spoofing - <numer RPT przedsiębiorcy telekomunikacyjnego>”.

D.2. Raportowanie[16)]

1. Na potrzeby rozliczalności i sprawozdawczości zaleca się, aby przedsiębiorca telekomunikacyjny był przygotowany do udostępnienia[17)] następujących informacji:
   1) zagregowanych dziennych danych o liczbie zrealizowanych połączeń głosowych;
   2) zagregowanych dziennych danych o liczbie połączeń głosowych, dla których została ukryta identyfikacja numeru wywołującego dla użytkownika końcowego w związku z realizacją obowiązku zwalczania CLI spoofing;
   3) zagregowanych dziennych danych o liczbie połączeń głosowych, które zostały zablokowane w związku z realizacją obowiązku zwalczania CLI spoofing
2. Na potrzeby rozliczalności i sprawozdawczości zaleca się, aby przedsiębiorca telekomunikacyjny realizujący tranzyt połączeń głosowych na łączach międzynarodowych był przygotowany do udostępnienia zagregowanych dziennych danych o liczbie połączeń głosowych prezentujących się numerami krajowymi, kierowanych do kraju poprzez łącza międzynarodowe na numery krajowe stacjonarne, jeżeli przedsiębiorca posiada łącza międzynarodowe[18)].

[16)] Do zapewnienia zdolności do oceny skuteczności rozwiązań stosowanych w walce z CLI spoofing niezbędne jest zdefiniowanie wskaźników podlegających statystyce. Dane statystyczne agregowane są w związku z realizacją postanowień art. 25 UZNKE oraz na podstawie art. 106 i art. 168 PT, zgodnie z którymi przedsiębiorca telekomunikacyjny jest obowiązany do rejestracji informacji o usługach telekomunikacyjnych, które nie zostały przez tego przedsiębiorcę wykonane w związku z realizacją walki z CLI spoofing.

[17)] Wzór raportu znajduje się w Biuletynie Informacji Publicznej Prezesa Urzędu Komunikacji Elektronicznej (plik Raport_CLI.xlsx w zakładce: Bezpieczeństwo).

[18)] Dotyczy zarówno połączeń głosowych przychodzących z numerów krajowych stacjonarnych jak i mobilnych.