|  |  |
| --- | --- |
| **Nazwa projektu**Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej**Ministerstwo wiodące i ministerstwa współpracujące**Kancelaria Prezesa Rady Ministrów**Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Janusz Cieszyński, Sekretarz Stanu w Kancelarii Prezesa Rady Ministrów**Kontakt do opiekuna merytorycznego projektu**Łukasz Wojewoda, Dyrektor Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl Marcin Wysocki, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa,e-mail: sekretariat.dc@mc.gov.pl  | **Data sporządzenia15.06.2022****Źródło:** Inicjatywa własna**Nr w wykazie prac**UD402 |
| **OCENA SKUTKÓW REGULACJI** |
| 1. **Jaki problem jest rozwiązywany?**
 |
| Komunikacja elektroniczna stanowi narzędzie powszechnie wykorzystywane w życiu codziennym przez współczesne społeczeństwo informacyjne. Z usług dostarczanych przez przedsiębiorców telekomunikacyjnych codziennie korzysta wiele milionów osób. Usługi te są również coraz szerzej i w sposób bardziej wyszukany wykorzystywane przez przestępców w celu wyrządzenia szkód po stronie przedsiębiorców telekomunikacyjnych, użytkowników końcowych lub osiągnięcie nienależnych korzyści.W ostatnich miesiącach nasiliły się również ataki na osoby fizyczne z wykorzystaniem usług telekomunikacyjnych[[1]](#footnote-1). Przestępcy, stosując specjalne bramki internetowe VoIP podszywali się pod numer zaufanych instytucji czy osoby publiczne i dzwonili z rzekomo prawdziwego numeru. W ten sposób próbowali nakłonić odbiorców do niekorzystnego działania czy w niektórych przypadkach nawet próbowali ich zastraszyć. Oszuści wykorzystywali w ten sposób słabości sieci telekomunikacyjnych, które powodują, że operatorzy sieci mobilnych 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. Zjawisko to występuje pod nazwą CLI spoofing.Innym zagrożeniem dla użytkowników są fałszywe krótkie wiadomości tekstowe SMS. Oszuści podszywając się pod zaufane instytucje próbują nakłonić nieświadome ofiary do ujawnienia danych osobowych, informacji o karcie kredytowej czy zainfekować urządzenie poprzez kliknięcie w link w wiadomości. Zjawisko to występuje pod nazwą smishingu.W tej sytuacji konieczne jest wprowadzenia odpowiednich przepisów dotyczących zwalczania nadużyć w komunikacji elektronicznej. Proponowane rozwiązania mają służyć stworzeniu odpowiednich ram prawnych do podejmowania działań w zakresie zapobiegania nadużyciom w komunikacji elektronicznej przez przedsiębiorców telekomunikacyjnych, a w dalszej perspektywie pozwolą w większym stopniu niż obecnie ograniczyć skalę nadużyć i chronić bezpieczeństwo użytkowników. |
| 1. **Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt**
 |
| Na przedsiębiorców telekomunikacyjnych zostaną nałożone obowiązki i uprawnienia związane z zwalczaniem nadużyć telekomunikacyjnych.Przedsiębiorcy telekomunikacyjnie będą obowiązani, w szczególności do:1. podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu przeciwdziałać nadużyciom w komunikacji elektronicznej;
2. blokowania krótkich wiadomości tekstowych, które zawierają treści o charakterze smishingu zgodne ze wzorcem wiadomości przekazanym przez CSIRT NASK;
3. blokowania połączeń głosowych, które mają na celu podszywanie się pod inną osobę lub instytucję.

Prezes Urzędu Komunikacji Elektronicznej będzie prowadził wykaz numerów służących wyłącznie do odbierania połączeń głosowych.Zespół CSIRT NASK będzie monitorował występowanie smishingu i przekazywał przedsiębiorcom telekomunikacyjnym wzorce wiadomości wskazujące na wystąpienie smishingu.Dostawcy poczty elektronicznej dla co najmniej 500 000 użytkowników, 500 000 aktywnych kont lub podmiotów publicznych będą obowiązani stosować mechanizm uwierzytelnienia poczty elektronicznej. |
| 1. **Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?**
 |
| W Wielkiej Brytanii OFCOM prowadzi listę numerów, z których nie są inicjowane połączenia. Są to numery m. in. instytucji publicznych np. infolinie dla obywateli.W Stanach Zjednoczonych przedsiębiorcy zostali zobowiązani na podstawie Telephone Robocall Abuse Criminal Enforcement and Deterrence Act oraz decyzji Federal Communication Commision do stosowania rozwiązania STIR/SHAKEN, które umożliwia uwierzytelnienie informacji adresowej połączenia[[2]](#footnote-2). |
| 1. **Podmioty, na które oddziałuje projekt**
 |
| Grupa | Wielkość | Źródło danych  | Oddziaływanie |
| CSIRT NASK | 1 | Informacja ogólnodostępna | Zespół CSIRT NASK będzie monitorował nadużycia w komunikacji elektronicznej oraz uruchomi system teleinformatyczny przekazujący wzorce wiadomości zawierające treści o charakterze smishingu. |
| Dostawcy poczty elektronicznej | brak danych |   | Dostawcy poczty elektronicznej dla co najmniej 500 000 użytkowników, 500 000 aktywnych kont lub podmiotów publicznych będą obowiązani stosować mechanizm uwierzytelnienia poczty elektronicznej. |
| Komendant Główny Policji | 1 | Informacja ogólnodostępna | Obowiązek podłączenia się do systemu teleinformatycznego przekazującego wzorce wiadomości zawierające treści o charakterze smishingu.  |
| Minister właściwy do spraw informatyzacji | 1 | Informacja ogólnodostępna | Minister właściwy do spraw informatyzacji będzie obowiązany zamieścić w Biuletynie Informacji Publicznej informację o uruchomieniu przez CSIRT NASK systemu teleinformatycznego przekazującego wzorce wiadomości zawierające treści o charakterze smishingu. |
| Prezes Urzędu Komunikacji Elektronicznej | 1 | Informacja ogólnodostępna | Obowiązek podłączenia się do systemu teleinformatycznego przekazującego wzorce wiadomości zawierające treści o charakterze nadużycia w komunikacji elektronicznej. Prezes UKE otrzyma również kompetencję do rozpatrywania sprzeciwu na zablokowanie komunikatu. Prezes UKE będzie również nakładał administracyjne kary pieniężne na przedsiębiorców telekomunikacyjnych za niestosowanie się do przepisów ustawy. Uzyska możliwość zawarcia z operatorami telekomunikacyjnymi porozumienia określającego środki organizacyjne i techniczne stosowanych przy przeciwdziałania CLI spoofing. |
| Przedsiębiorcy telekomunikacyjni | 4017 | Rejestr przedsiębiorców telekomunikacyjnych |  Na przedsiębiorców telekomunikacyjnych zostaną nałożone obowiązki i uprawnienia związane z zwalczaniem nadużyć w komunikacji elektronicznej. |
| 1. **Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji**
 |
| W ramach 14 - dniowych konsultacji i opiniowania projekt zostanie skierowany do zaopiniowania przez:1. American Chamber of Commerce in Poland;
2. Busines Centre Club;
3. Federacja Konsumentów;
4. Fundacja Bezpieczna Przestrzeń;
5. Fundacja im. Kazimierza Pułaskiego;
6. Fundacja im. Stefana Batorego;
7. Fundacja Instytut Mikromakro;
8. Fundacja Moje Państwo;
9. Fundacja MY Pacjenci;
10. Fundacja Nowoczesna Polska;
11. Fundacja Panoptykon;
12. Fundacja Projekt: Polska;
13. Interdyscyplinarne Centrum Modelowania Matematycznego i Komputerowego UW;
14. Izba Gospodarki Elektronicznej;
15. Klaster #CyberMadeInPoland;
16. Konfederacja Lewiatan;
17. Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji;
18. Krajowa Izba Gospodarcza;
19. Krajowa Izba Gospodarki Cyfrowej;
20. Krajowa Izba Gospodarki Morskiej;
21. Krajowa Izba Komunikacji Ethernetowej;
22. Krajowa Izba Rozliczeniowa S.A.;
23. Krajowe Stowarzyszenie Ochrony Informacji Niejawnych;
24. Naczelna Organizacja Techniczna;
25. Naczelna Rada Zrzeszeń Handlu i Usług;
26. Ogólnopolskie Porozumienie Organizacji Radioamatorskich;
27. PKP TELKOL sp. z o.o.;
28. Polska Federacja Szpitali;
29. Polska Izba Handlu;
30. Polska Izba Informatyki i Telekomunikacji;
31. Polska Izba Komunikacji Elektronicznej;
32. Polska Izba Producentów Urządzeń i Usług na Rzecz Kolei;
33. Polska Izba Radiodyfuzji Cyfrowej;
34. Polska Organizacja Handlu i Dystrybucji;
35. Polska Organizacja Niebankowych Instytucji Płatności;
36. Polska Rada Biznesu;
37. Polska Wytwórnia Papierów Wartościowych;
38. Polski Związek Krótkofalowców;
39. Polski Związek Pracodawców Przemysłu Farmaceutycznego;
40. Polskie Centrum Badań i Certyfikacji S.A.;
41. Polskie Górnictwo Naftowe i Gazownictwo;
42. Polskie Koleje Państwowe S.A.;
43. Polskie Stowarzyszenie Marketingu SMB;
44. Polskie Towarzystwo Informatyczne;
45. Polskie Związek Przemysłu Motoryzacyjnego;
46. SABI – stowarzyszenie inspektorów ochrony danych;
47. Sieć Obywatelska Watchdog Polska;
48. Stowarzyszenie „Archiwizjoner”;
49. Stowarzyszenie Inżynierów Telekomunikacji;
50. Stowarzyszenie ISACA;
51. Towarzystwo Gospodarcze Polskie Elektrownie;
52. Związek Banków Polskich;
53. Związek Importerów i Producentów Sprzętu Elektrycznego i Elektronicznego – ZIPSEE Cyfrowa Polska;
54. Związek Pracodawców Branży Internetowej IAB Polska;
55. Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM;
56. Związek Pracodawców Mediów Publicznych;
57. Związek Przedsiębiorców i Pracodawców;
58. Związek Telewizji Kablowych w Polsce – Izba Gospodarcza.
59. Prezesa Urzędu Komunikacji Elektronicznej;
60. Prezesa Urzędu Ochrony Danych Osobowych;
61. Prezesa Urzędu Ochrony Konkurencji i Konsumentów.

Stosownie do art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) oraz art. 52 § 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2022 r. poz. 348) projekt ustawy został udostępniony w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji w serwisie Rządowy Proces Legislacyjny. |
| 1. **Wpływ na sektor finansów publicznych**
 |
| (ceny stałe z …… r.) | Skutki w okresie 10 lat od wejścia w życie zmian [mln zł] |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | *Łącznie (0-10)* |
| **Dochody ogółem** |  |  |  |  |  |  |  |  |  |  |  |  |
| budżet państwa |  |  |  |  |  |  |  |  |  |  |  |  |
| JST |  |  |  |  |  |  |  |  |  |  |  |  |
| pozostałe jednostki (oddzielnie) |  |  |  |  |  |  |  |  |  |  |  |  |
| **Wydatki ogółem** |  |  |  |  |  |  |  |  |  |  |  |  |
| budżet państwa |  |  |  |  |  |  |  |  |  |  |  |  |
| JST |  |  |  |  |  |  |  |  |  |  |  |  |
| pozostałe jednostki (oddzielnie) |  |  |  |  |  |  |  |  |  |  |  |  |
| **Saldo ogółem** |  |  |  |  |  |  |  |  |  |  |  |  |
| budżet państwa |  |  |  |  |  |  |  |  |  |  |  |  |
| JST |  |  |  |  |  |  |  |  |  |  |  |  |
| pozostałe jednostki (oddzielnie) |  |  |  |  |  |  |  |  |  |  |  |  |
| Źródła finansowania  | Przyjęte rozwiązania nie spowodują dodatkowych skutków finansowych dla sektora finansów publicznych, w tym budżetu państwa i budżetów jednostek samorządu terytorialnego   |
| Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń |  |
| 1. **Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe**
 |
| Skutki |
| Czas w latach od wejścia w życie zmian | 0 | 1 | 2 | 3 | 5 | 10 | *Łącznie (0-10)* |
| W ujęciu pieniężnym(w mln zł, ceny stałe z …… r.) | duże przedsiębiorstwa |  |  |  |  |  |  |  |
| sektor mikro-, małych i średnich przedsiębiorstw |  |  |  |  |  |  |  |
| rodzina, obywatele oraz gospodarstwa domowe |  |  |  |  |  |  |  |
| (dodaj/usuń) |  |  |  |  |  |  |  |
| W ujęciu niepieniężnym | duże przedsiębiorstwa | Przedsiębiorcy telekomunikacyjni będą obowiązani do podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczaniu.Dostawcy poczty elektronicznej dla co najmniej 500 000 użytkowników, 500 000 aktywnych kont lub podmiotów publicznych będą obowiązani stosować mechanizm uwierzytelnienia poczty elektronicznej. |
| sektor mikro-, małych i średnich przedsiębiorstw | Mikro, mali i średni przedsiębiorcy telekomunikacyjni będą obowiązani do podejmowania proporcjonalnych technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie. |
| rodzina, obywatele oraz gospodarstwa domowe  | Projekt ustawy przełoży się na zwiększenie bezpieczeństwa usług komunikacji elektronicznej świadczonych dla obywateli. Utrudni przestępcom podszywanie się pod inne osoby i oszukiwanie obywateli. |
| (dodaj/usuń) |  |
| Niemierzalne | (dodaj/usuń) |  |
| (dodaj/usuń) |  |
| Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń  |  |
| 1. **Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu**
 |
| [ ]  nie dotyczy |
| Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności). | [ ]  tak[ ]  nie[x]  nie dotyczy |
| [ ]  zmniejszenie liczby dokumentów [ ]  zmniejszenie liczby procedur[ ]  skrócenie czasu na załatwienie sprawy[ ]  inne: … | [x]  zwiększenie liczby dokumentów[x]  zwiększenie liczby procedur[ ]  wydłużenie czasu na załatwienie sprawy[ ]  inne: … |
| Wprowadzane obciążenia są przystosowane do ich elektronizacji.  | [x]  tak[ ]  nie[ ]  nie dotyczy |
| Komentarz:Ustawa wprowadza następujące obowiązki na przedsiębiorców telekomunikacyjnych:1. podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie;
2. podłączenie się do systemu teleinformatycznego przekazującego wzorce wiadomości o charakterze smishingu;
3. niezwłoczne blokowanie krótkich wiadomości tekstowych zawierających treści zawarte we wzorcu wiadomości;
4. blokowanie lub ukrycie identyfikacji numeru wywołującego dla użytkownika końcowego w przypadku wystąpienia CLI spoofingu;
5. rejestracja danych o usługach telekomunikacyjnych, które nie zostały wykonane z uwagi na blokowanie krótkich wiadomości tekstowych.

Dostawcy poczty elektronicznej dla co najmniej 500 000 użytkowników, 500 000 aktywnych kont lub podmiotów publicznych będą obowiązani stosować mechanizmy uwierzytelnienia poczty elektronicznej. |
| 1. **Wpływ na rynek pracy**
 |
| Projekt może wygenerować potrzebę zatrudnienia przez niektórych przedsiębiorców telekomunikacyjnych specjalistów do obsługi systemów wykrywania i zwalczania nadużyć w komunikacji elektronicznej.  |
| 1. **Wpływ na pozostałe obszary**
 |
| [ ]  środowisko naturalne[ ]  sytuacja i rozwój regionalny[x]  sądy powszechne, administracyjne lub wojskowe | [ ]  demografia[ ]  mienie państwowe[ ]  inne:       | [x]  informatyzacja[ ]  zdrowie |
| Omówienie wpływu | Projekt spowoduje powstanie:* nowego systemu teleinformatycznego służącego do wymiany informacji o wzorcach wiadomości o charakterze smishingu;
* wykazu numerów służących wyłącznie do odbierania połączeń głosowych.

Ustawa wprowadza administracyjne kary za niedostosowanie się do obowiązków wynikających z jej przepisów. Skargi na decyzje administracyjne o nałożeniu kary będą rozpatrywane przez sądy administracyjne. Trudno jest oszacować ile może być nałożonych kar, a co za tym idzie nie jest możliwe oszacowanie liczby postępowań sądowoadministracyjnych wszczętych na podstawie skarg na te decyzje. |
| 1. **Planowane wykonanie przepisów aktu prawnego**
 |
| Ustawa wejdzie w życie po upływie 30 dni od dnia ogłoszenia. W terminie 3 miesięcy od dnia wejścia w życie ustawy zespół CSIRT NASK uruchomi system teleinformatyczny służący do przekazywania wzorców wiadomości o charakterze smishingu i poinformuje o tym ministra właściwego do spraw informatyzacji. Minister z kolei niezwłocznie po otrzymaniu informacji z CSIRT NASK zamieści informację o uruchomieniu tego systemu w Biuletynie Informacji Publicznej. Po opublikowaniu tej informacji Komendant Główny Policji, Prezes Urzędu Komunikacji Elektronicznej oraz przedsiębiorcy telekomunikacyjni będą obowiązani podłączyć się do tego systemu w terminie 3 miesięcy.Przedsiębiorcy telekomunikacyjni będą obowiązani podjąć proporcjonalne środki techniczne i organizacyjne mające na celu zapobieganie i zwalczanie: smishingu – w terminie 6 miesięcy od dnia wejścia w życie ustawy oraz CLI spoofingu – w terminie 12 miesięcy od dnia wejścia w życie ustawy. |
| 1. **W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?**
 |
| Ewaluacja efektów projektu nastąpi po roku. Zostaną zastosowane następujące mierniki:* liczba numerów wpisanych do wykazu numerów służących wyłącznie do odbierania połączeń głosowych,
* liczba wzorców wiadomości o charakterze smishingu przekazanych przez CSIRT NASK do przedsiębiorców telekomunikacyjnych.
 |
| 1. **Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)**
 |
| Brak |

1. Raport roczny z działalności CERT Polska Krajobraz bezpieczeństwa polskiego Internetu 2021 str 81

https://cert.pl/uploads/docs/Raport\_CP\_2021.pdf [↑](#footnote-ref-1)
2. <https://www.fcc.gov/document/mandating-stirshaken-combat-spoofed-robocalls-0> [↑](#footnote-ref-2)