



Wiceprezes Rady Ministrów Minister Cyfryzacji

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Krzysztof Gawkowski

DC.WAC.5555.96.2026

Warszawa, 04 września 2026 r.

Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa nr 2026-76-7

dotycząca ochrony kont w komunikatorze Signal przed przejęciem z wykorzystaniem klucza odzyskiwania kopii zapasowej

Wstęp

Niniejsza rekomendacja została wydana na podstawie art. 67a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa¹ (ustawa o KSC). Jej celem jest podniesienie poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa (KSC) w związku z identyfikacją nowej odłogi kampanii socjotechnicznej wymierzonej w użytkowników komunikatora Signal.

Niniejsza rekomendacja stanowi uzupełnienie rekomendacji Pełnomocnika Rządu ds. Cyberbezpieczeństwa dotycząca komunikatora Signal z dnia 13.05.2026 roku².

Rekomendacja

Atakujący w obserwowanym wariantcie kampanii podszywają się pod oficjalne konto **Signal Support** i nakłaniają użytkowników do uruchomienia mechanizmu tworzenia kopii zapasowej na serwerze Signal, a następnie do przekazania lub przesłania **64-znakowego klucza odzyskiwania**.

Pozyskanie przez atakującego tego klucza umożliwia przejęcie konta użytkownika oraz odszyfrowanie zawartości kopii zapasowej, w tym dostęp do historycznych wiadomości i multimediów wymienianych z poszczególnymi kontaktami. Szczególnie narażone na tego rodzaju działania są osoby zajmujące kierownicze stanowiska w administracji publicznej, osoby pełniące funkcje publiczne, kadra zarządzająca spółek oraz kierownictwo podmiotów KSC.

Tego rodzaju incydenty stanowią istotne zagrożenie dla poufności komunikacji oraz mogą prowadzić do pozyskania przez podmioty nieuprawnione wrażliwych informacji dotyczących funkcjonowania podmiotów kluczowych i podmiotów ważnych, w tym administracji publicznej.

Podstawowe zasady bezpieczeństwa

W związku z obserwowaną kampanią rekomenduję stosowanie następujących zasad:

- nigdy nie przekazywać osobom trzecim kodów weryfikacyjnych SMS wykorzystywanych przez Signal;

¹ Dz.U. z 2026 r. poz. 20 z późn. zm.

² <https://www.gov.pl/web/cyfryzacja/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-dotyczaca-komunikatora-signal>

- nigdy nie udostępniać kodu PIN Signal;
- nigdy nie przekazywać ani nie przysyłać 64-znakowego klucza odzyskiwania kopii zapasowej Signal (przekazanie kodu pozwala na przejęcie wszystkich historycznych wiadomości, a także multimediów z ostatnich 45 dni);
- pamiętać, że pracownicy Signal ani konto Signal Support nie proszą użytkowników o przekazanie klucza odzyskiwania;
- zachować szczególną ostrożność wobec wiadomości nakłaniających do wykonania kopii zapasowej lub weryfikacji konta;
- regularnie sprawdzać listę powiązanych urządzeń w ustawieniach komunikatora;
- aktywować funkcję „Blokada rejestracji” oraz pozostałe mechanizmy zwiększające bezpieczeństwo konta;
- rozważyć wyłączenie funkcji przechowywania kopii zapasowych na serwerach Signal, jeżeli nie jest ona niezbędna do realizacji potrzeb użytkownika;
- nie wykorzystywać komunikatora Signal do przekazywania informacji niejawnych oraz innych informacji, których ujawnienie mogłoby powodować negatywne skutki dla bezpieczeństwa podmiotu.

Postępowanie w przypadku podejrzenia kompromitacji klucza odzyskiwania

Jeżeli istnieje podejrzenie, że klucz odzyskiwania został ujawniony lub przekazany osobie nieuprawnionej, zaleca się niezwłocznie:

- zmianę kodu PIN Signal (*Ustawienia>Konto>Zmień swój kod PIN*);
- usunięcie istniejącej kopii zapasowej zapisanej na serwerze Signal (*Ustawienia>Kopie zapasowe>Pokaż Ustawienia>Usuń kopie zapasowe i wyłącz*);
- wyłączenie mechanizmu automatycznego tworzenia nowych kopii zapasowych;
- wygenerowanie nowego klucza odzyskiwania przed utworzeniem kolejnej kopii zapasowej (*Ustawienia>Kopie zapasowe>Pokaż Ustawienia>Wyświetl kod odzyskiwania>Utwórz nowy kod*);
- zgłoszenie incydentu do właściwego zespołu odpowiedzialnego za cyberbezpieczeństwo.

Incydenty dotyczące urządzeń prywatnych należy zgłaszać do zespołu reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego CSIRT NASK³.

W przypadku urządzeń służbowych zgłoszenie powinno zostać przekazane zgodnie z procedurami obowiązującymi w danej organizacji, a komórka odpowiedzialna za cyberbezpieczeństwo w danej organizacji powinno zgłosić incydent do właściwego zespołu CSIRT.

Rekomendowane narzędzia komunikacji służbowej

³ Zgodnie z art. 26 ust. 6 pkt 1 lit. I ustawy o KSC CSIRT NASK jest właściwy w zakresie koordynacji obsługi incydentów zgłaszanych osoby fizyczne. Informacja o dostępnych formach zgłoszenia incydentu dostępna jest na stronie CERT Polska, działającego w strukturze CSIRT NASK: <https://incydent.cert.pl/>.

W celu ograniczenia ryzyk wynikających z korzystania z komercyjnych komunikatorów internetowych do komunikacji służbowej rekomenduje się wykorzystywanie narzędzi udostępnianych przez Ministerstwo Cyfryzacji i NASK-PIB, w szczególności:

1. Komunikator mSzyfr

mSzyfr jest rekomendowanym rozwiązaniem przeznaczonym do bezpiecznej szyfrowanej komunikacji służbowej dla administracji publicznej.

2. System łączności niejawnej SKR-Z

System przeznaczony do realizacji łączności niejawnej dla administracji publicznej funkcjonujący w środowisku odseparowanym od Internetu.

Zalecenia końcowe

Ze względu na rosnącą aktywność zaawansowanych kampanii socjotechnicznych zaleca się prowadzenie działań podnoszących świadomość użytkowników w zakresie ochrony komunikacji elektronicznej oraz regularne szkolenia z zakresu cyberbezpieczeństwa, w szczególności dla osób pełniących funkcje kierownicze i posiadających dostęp do informacji o podwyższonej wrażliwości.

Mimo, iż tworzenie kopii zapasowej na serwerze Signal jest wygodne dla użytkownika, należy mieć na uwadze, że mechanizm ten otwiera potencjalny wektor ataku umożliwiający przejęcie treści historycznych wiadomości. Dlatego podczas korzystania z tej opcji zaleca się szczególną ostrożność w sposobie prawidłowego zarządzania kluczem odzyskiwania, tj. nieudostępniania i nieprzesyłania go osobom trzecim. Klucz ten stanowi krytyczny mechanizm odpowiedzialny za bezpieczeństwo konta użytkownika aplikacji Signal.

Rekomendacja została opracowana w ramach współpracy Ministerstwa Cyfryzacji i zespołu CSIRT GOV.

Krzysztof Gawkowski

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa

Wiceprezes Rady Ministrów

Minister Cyfryzacji

/dokument podpisany elektronicznie/

