Wiceprezes Rady Ministrów
Minister Cyfryzacji

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Krzysztof Gawkowski

DC.WAC.5555.27.2026
Warszawa, 13 maja 2026

Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa dotycząca ograniczenia ryzyk związanych z korzystaniem z komunikatora Signal

Niniejsza rekomendacja została wydana na podstawie art. 67a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[1]. Jej celem jest podniesienie poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa (KSC), w związku z utrzymującym się wysokim poziomem zagrożeń oraz wzmożonych ataków wymierzonych w użytkowników aplikacji Signal na terenie Rzeczypospolitej Polskiej.

Zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) poziomu krajowego w sposób ciągły identyfikują i analizują kampanie phishingowe prowadzone przez zaawansowane technicznie grupy typu APT, powiązane ze służbami wrogich państw. Charakter, skala oraz stopień koordynacji tych działań wskazują, że pozostają one ukierunkowane przede wszystkim na osoby zajmujące eksponowane stanowiska publiczne oraz pracowników instytucji publicznych.

Celem tych działań jest przejęcie kontroli nad kontami użytkowników komunikatora Signal, w szczególności poprzez podszywanie się pod obsługę techniczną aplikacji oraz nakłanianie do kliknięcia w złośliwe odnośniki pod pretekstem rzekomego zablokowania konta. Tego rodzaju incydenty stanowią istotne i bezpośrednie zagrożenie dla poufności, integralności oraz bezpieczeństwa komunikacji prowadzonej przez osoby pełniące funkcje publiczne, a pośrednio również dla bezpieczeństwa obywateli.

Podstawowe zasady bezpieczeństwa

W nawiązaniu do wcześniejszych komunikatów Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa przypominam o bezwzględnej konieczności stosowania następujących zasad w przypadku otrzymania podejrzanej wiadomości o blokadzie konta, konieczności weryfikacji w aplikacji Signal oraz podczas jej codziennego użytkowania:

- nie klikać w linki znajdujące się w nieoczekiwanych SMS, e-mailach itp.;
- nigdy nie udostępniać nikomu kodów weryfikacyjnych SMS ani numeru PIN;
- pamiętać, że dział obsługi klienta aplikacji Signal nigdy nie kontaktuje się z użytkownikami bezpośrednio poprzez wiadomości w komunikatorze;
- skanować kody QR wyłącznie za pomocą aplikacji Signal;
- regularnie weryfikować listę powiązanych urządzeń w ustawieniach konta Signal;
- aktywować funkcję „Blokada rejestracji”, która wymaga dodatkowej autoryzacji;

[1] Dz. U. z 2026 r. poz. 20, z późn. zm. (dalej jako: ustawa o KSC).

telefon: +48 22 245 54 42
adres email: sekretariat.BM@cyfra.gov.pl
adres strony internetowej: www.gov.pl/cyfryzacja

adres: ul. Królewska 27
00-060 Warszawa

- uruchomić ustawienia prywatności - ukrycie własnego numeru telefonu w aplikacji i posługiwaniu się unikalną nazwą użytkownika;
- nie używać komunikatora do przesyłania informacji niejawnych ani wrażliwych;
- niezwłocznie zgłosić incydent:
    - na urządzeniach prywatnych – do CSIRT NASK[2] za pośrednictwem strony https://incydent.cert.pl;
    - na urządzeniach służbowych – do wewnętrznej komórki odpowiedzialnej za cyberbezpieczeństwo, która powinna przekazać zgłoszenie do właściwego zespołu CSIRT[3].

W załączeniu do niniejszej rekomendacji zawarte są zalecenia Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni (DKWOC) w sprawie wykorzystania i konfiguracji komunikatora Signal, których zastosowanie znacząco pozwoli podnieść poziom bezpieczeństwa wykorzystania komunikatora Signal.

Rekomendowane, zaufane narzędzia komunikacji służbowej dla administracji publicznej

W celu ograniczenia ryzyk wynikających z korzystania z komercyjnych komunikatorów internetowych w komunikacji służbowej, zaleca się wykorzystywanie narzędzi udostępnianych przez Ministerstwo Cyfryzacji, które we współpracy z Naukową i Akademicką Siecią Komputerową – Państwowym Instytutem Badawczym (NASK-PIB), zapewnia nieodpłatny dostęp do zaufanych systemów komunikacji służbowej, spełniających wymogi bezpieczeństwa, w szczególności:

1. **Bezpieczny komunikator mSzyfr[4]:**

   Komunikator mSzyfr jest rekomendowanym narzędziem do prowadzenia bezpiecznej komunikacji służbowej. Rozwiązanie to przeznaczone jest dla:

   - podmiotów administracji publicznej;
   - podmiotów krajowego systemu cyberbezpieczeństwa, ujętych w wykazie podmiotów kluczowych i ważnych;
   - innych podmiotów – po uzyskaniu zgody Ministra Cyfryzacji.

2. **System łączności niejawnej SKR-Z:**

   - system SKR-Z przeznaczony jest do realizacji łączności niejawnej (do klauzuli „ZASTRZEŻONE”, „RESTREINT UE/EU RESTRICTED”, „NATO RESTRICTED” i funkcjonuje w środowisku wyizolowanym od Internetu.

Zarówno komunikator mSzyfr, jak i system SKR-Z pozostają w całości pod jurysdykcją Rzeczypospolitej Polskiej. Infrastruktura teleinformatyczna obsługująca te rozwiązania jest zlokalizowana na terytorium Rzeczypospolitej Polskiej i administrowana przy zapewnieniu odpowiednich standardów cyberbezpieczeństwa.

[2] CSIRT NASK jest właściwy w przypadku zgłoszeń od osób fizycznych.
[3] Zgodnie z art. 26 ust. 5-7 ustawy o KSC.
[4] https://www.gov.pl/web/baza-wiedzy/komunikator-mszyfr

Zalecam również kadrze kierowniczej administracji publicznej udział w skierowanych do niej indywidualnych szkoleniach SecureV[5], obejmujących m.in. zagadnienia z zakresu higieny cyfrowej oraz ochrony przed phishingiem.

Niniejsza rekomendacja została opracowana przy współpracy Ministerstwa Cyfryzacji oraz CSIRT MON.

Załącznik nr 1: Zalecenia DKWOC w sprawie wykorzystania i konfiguracji komunikatora Signal

Krzysztof Gawkowski
Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Wiceprezes Rady Ministrów
Minister Cyfryzacji
/dokument podpisany elektronicznie/

[5] https://www.nask.pl/instytut/dla-instytucji/secure-v