Ministerstwo Cyfryzacji

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa

DC.WAC.5555.30.2026
Warszawa, 25 czerwca 2026

Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa

nr 2026/67a/4

dotycząca ograniczenia ryzyk związanych z transportem poczty z wykorzystaniem nieszyfrowanych kanałów transmisji

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 zagrożeniem ujawnienia korespondencji pocztowej podczas jej transportu poprzez sieć Internet pomiędzy serwerami pocztowymi wykorzystującymi nieszyfrowane kanały transmisji.

Wprowadzenie

Poczta elektroniczna, czyli popularny e-mail, to usługa sieciowa umożliwiająca przesyłanie wiadomości i plików między użytkownikami Internetu. Komunikacja ta może odbywać się na dwa sposoby: kanałem jawnym lub szyfrowanym. W przypadku tradycyjnego, jawnego połączenia treść e-maila jest przesyłana otwartym tekstem, co naraża je na przechwycenie przez osoby trzecie. Z kolei użycie protokołów szyfrujących (takich jak TLS) zabezpiecza transmisję.

Rekomendacja

Brak skonfigurowanego TLS sprawia, że transmisja poczty może odbywać się w postaci jawnej, co zwiększa ryzyko przechwycenia korespondencji, a także otwiera infrastrukturę na ataki Man in the Middle[2]. W związku z powyższym rekomenduję wdrożenie niżej wymienionych zaleceń:

- konfiguracja serwerów pocztowych powinna również umożliwiać sprawdzanie poprawności prezentowanych certyfikatów, tak aby systemy wysyłające pocztę sprawdzały ich ważność, zaufanie oraz zgodność z nazwą „hosta”.
- ustawienia rekordów PTR dla serwerów pocztowych w usłudze DNS, aby wesprzeć ocenę wiarygodności nadawcy przez filtry antyspamowe, co może ograniczyć ryzyko oznaczenia prawidłowej korespondencji jako spam,
- wyłączenie słabych algorytmów szyfrowania i protokołów kryptograficznych[3] (m.in. RC4, DES, 3DES, wszystkich wersji SSL oraz TLS 1.0, 1.1),

[1] Dz. U. z 2026 r. poz. 20, z późn. zm. (dalej jako: ustawa o KSC).
[2] Man-in-the-Middle (MitM) – atak polegający na nieautoryzowanym pośredniczeniu w komunikacji między dwoma podmiotami, umożliwiający podsłuchiwanie, przechwytywanie oraz manipulację przesyłanymi danymi bez wiedzy uczestników komunikacji
[3] Lista uznawanych za słabe algorytmów i protokołów kryptograficznych ulega zmianom w czasie wraz z rozwojem metod kryptanalizy oraz rekomendacji krajowych zespołów CSIRT.

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

— wykorzystanie certyfikatów wystawionych przez zaufane urzędy certyfikacji CA[4] (np. z listy zaufanych dostawców prowadzonej przez Komisję Europejską).

CSIRT NASK poszerzył zakres oferowanych usług portalu bezpiecznapoczta.cert.pl[5] o moduł sprawdzający, czy serwery pocztowe obsługują szyfrowanie komunikacji. Dodatkowo w ramach projektu Artemis[6] cykliczne skanowanie będzie obejmowało również sprawdzenie czy serwery pocztowe umożliwiają zestawienie połączenia szyfrowanego.

Rekomendacja została opracowana dzięki współpracy Ministerstwa Cyfryzacji oraz CSIRT NASK, CSIRT MON i CSIRT GOV.

Z wyrazami szacunku

z up. Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa
Łukasz Wojewoda
Dyrektor
Departamentu Cyberbezpieczeństwa
w Ministerstwie Cyfryzacji

/dokument podpisany elektronicznie/

[4] Zaufany urząd certyfikacji (CA) – podmiot wydający certyfikaty potwierdzające tożsamość stron w komunikacji TLS/SSL. EU Trusted Lists (EUTL) – europejska lista zaufanych dostawców usług zaufania. https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls
[5] https://bezpiecznapoczta.cert.pl/
[6] https://cert.pl/skanowanie/