Wiceprezes Rady Ministrów
Minister Cyfryzacji

**Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa**
Krzysztof Gawkowski

DC.WAC.5555.37.2026

Warszawa, $data podpisu r.

**Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa**

**nr 2026/67a/3**

**dotycząca przeciwdziałania atakom ransomware**

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 zakresie przeciwdziałania cyberatakom typu ransomware.

## Wprowadzenie

Ransomware to rodzaj złośliwego oprogramowania (malware), którego celem jest szyfrowanie plików na urządzeniu. Efektem infekcji jest to, że zarówno same pliki, jak i systemy od nich zależne stają się bezużyteczne, a następnie cyberprzestępcy żądają okupu w zamian za odszyfrowanie danych.

Z biegiem czasu atakujący udoskonalili swoje techniki, czyniąc je bardziej destrukcyjnymi i dotkliwymi, zaczęli również wykradać dane ofiar i wywierać presję poprzez groźbę ich publikacji (tzw. „podwójne wymuszenie" – double extortion). Tego typu ataki oraz powiązane naruszenia danych mogą poważnie zakłócić funkcjonowanie organizacji. Zablokowany dostęp do kluczowych informacji niezbędnych do prowadzenia działalności i świadczenia krytycznych usług często wywołuje skutki ekonomiczne i wizerunkowe. Proces odzyskiwania sprawności po infekcji jest często długotrwały i kosztowny, jeżeli nie zostały podjęte kroki, które mogą przygotować organizację na tego typu ataki.

Połączone Centrum Operacyjne Cyberbezpieczeństwa (PCOC) otrzymuje informacje od zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) poziomu krajowego o infekcjach oprogramowaniem ransomware. W celu przeciwdziałania poszerzającemu się zjawisku Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa zdecydował o przygotowaniu rekomendacji dla podmiotów Krajowego Systemu Cyberbezpieczeństwa (KSC) w sprawie przeciwdziałania tego rodzaju zagrożeniom i zmniejszeniu ryzyka wystąpienia incydentu krytycznego.

[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

**Rekomendacja**

Ze względu na popularność ataków ransomware oraz możliwość wystąpienia incydentu krytycznego rekomendowane jest podjęcie poniższych działań oraz stosowanie ich regularnie:

1. Regularne utrzymywanie kopii zapasowych danych oraz najważniejszych systemów:
   - Cykliczne tworzenie kopii zapasowych z wykorzystaniem zasady 3:2:1, polegającej na utrzymywaniu minimum trzech pełnych kopii danych, z wykorzystaniem dwóch odmiennych technologii zapisu lub platform oraz przechowywanie minimum jednej kopii zapasowej poza głównym ośrodkiem serwerowni,
   - Posiadanie sprawdzonych i regularnie aktualizowanych obrazów maszyn referencyjnych (tzw. golden image) pozwalających na bezpieczne i sprawne odtworzenie infrastruktury w razie wystąpienia incydentu,
   - Zapis kopii zapasowych na nośnikach jednokrotnego zapisu w technologii Write Once Read Many,
   - Cykliczna weryfikacja poprawności tworzonych kopii zapasowych oraz sprawdzanie czy procedury odtwarzania systemu po ataku są skuteczne.
2. Zarządzanie dostępem:
   - Ograniczenie dostępu zdalnego i usług transferu danych dostępnych z sieci zewnętrznej do koniecznego minimum. W przypadku potrzeby ich dostępności, zabezpieczenie dostępu poprzez usługę VPN z wykorzystaniem wieloskładnikowego uwierzytelnienia,
   - Wdrożenie wieloskładnikowego uwierzytelnienia we wszystkich usługach i serwisach, w których jest to możliwe,
   - Zapewnienie segmentacji sieci w oparciu o przeznaczenie i krytyczność systemów (m. in. wydzielenie sieci biurowej i dla klientów),
   - Automatyczne blokowanie kont użytkowników w przypadku kilkukrotnego podania błędnych poświadczeń logowania,
   - Stosowanie zasady minimalnych uprawnień – "least privilege" i weryfikacja czy użytkownicy w systemie posiadają uprawnienia dostosowane do wykonywanej pracy. Wykorzystywanie dedykowanych kont o niższych uprawnieniach na potrzeby aplikacji działających w systemie,
   - Monitorowanie znanych wycieków haseł pod kątem wystąpienia w nich poświadczeń wykorzystywanych w organizacji i natychmiastowa reakcja w przypadku wycieku (np. blokada konta użytkownika, zmiana hasła),
   - Ograniczenie dostępu do kontrolera domeny dopuszczające połączenia wyłącznie z wybranych hostów z sieci wewnętrznej,
   - Modyfikowanie użytkowników w usłudze Active Directory wyłącznie podczas dedykowanego okna serwisowego.
3. Organizacja pracy:
   - Wdrożenie i doskonalenie procedur postępowania w przypadku wystąpienia incydentu cyberbezpieczeństwa,

- Wyznaczenie osoby do kontaktów oraz jej zastępców do komunikacji w przypadku zaistnienia incydentu,
- Reagowanie na informacje przekazywane przez zespoły CSIRT,
- Regularne szkolenia pracowników w zakresie dobrych praktyk i cyberhigieny oraz podnoszenie kompetencji pracowników IT.

4. Inwentaryzacja i monitorowanie zasobów:
   - Cykliczna inwentaryzacja zasobów, usług i urządzeń oraz ich konfiguracji, w tym utrzymywanie aktualnego schematu infrastruktury,
   - Wyłączenie niewykorzystywanych portów, usług i urządzeń,
   - Regularna aktualizacja komponentów infrastruktury,
   - Monitorowanie publikowanych podatności dotyczących wykorzystywanych narzędzi i natychmiastowe podejmowanie działań mitygujących zagrożenie,
   - Monitorowanie infrastruktury oraz gromadzenie i analizowanie logów z urządzeń brzegowych pod kątem wystąpienia anomalii, również z wykorzystaniem agregatorów logów (np. SIEM),
   - Cykliczna weryfikacja poprawnego zapisu i transportu logów.

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

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