Wiceprezes Rady Ministrów
Minister Cyfryzacji

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Krzysztof Gawkowski

DC.WAC.5555.50.2026
Warszawa, 21 lipca 2026

Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa

nr 2026/67a/6

dotycząca utrzymywania i konfiguracji urządzeń brzegowych

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 popularnością ataków na urządzenia brzegowe i ich wpływem na bezpieczeństwo dotkniętego incydentem podmiotu, a pośrednio także na inne podmioty KSC.

Wprowadzenie

Urządzenia brzegowe stanowią jeden z najczęstszych celów ataków, co niesie ze sobą poważne ryzyko paraliżu kluczowej infrastruktury. Aby skutecznie zminimalizować ryzyko wystąpienia incydentów na urządzeniach brzegowych, rekomenduje się podjęcie kompleksowych działań zabezpieczających.

Rekomendacja

Aby zmniejszyć ryzyko wystąpienia ataku na urządzenia brzegowe, rekomenduję wdrożenie niżej wymienionych zaleceń.

1. Zarządzanie urządzeniami
    - Utrzymywanie spisu urządzeń brzegowych zawierającego informacje dotyczące rodzajów urządzeń, wykorzystywanych wersji oprogramowania, skonfigurowanych połączeniach wewnętrznych i zewnętrznych między urządzeniami oraz usługach i portach udostępnionych publicznie w sieci internet.
    - Cykliczna inwentaryzacja i aktualizacja spisu urządzeń brzegowych.
    - Cykliczna aktualizacja oprogramowania.
    - Wdrożenie procedur wymiany urządzeń, które przestały być rozwijane (End of Life) i dla których zakończyło się wsparcie producenta (End of Service Life).
    - Wdrożenie procedur odtworzenia infrastruktury po ataku zmniejszających ryzyko ponownego incydentu, m. in:
        - Tworzenie nowej konfiguracji urządzenia z użyciem zweryfikowanych i niezbędnych elementów konfiguracji, bez bezpośredniego kopiowania całych bloków.
        - Weryfikacja obecności nieautoryzowanych kont użytkowników.

[1] Dz. U. z 2026 r. poz. 20, z późn. zm.

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

- Ponowna instalacja firmware udostępnianego bezpośrednio przez producenta.

2. Zarządzanie dostępem
    - Wyłączenie dostępu do panelu administracyjnego urządzenia bezpośrednio z sieci internet.
    - Ograniczenie dostępu zdalnego do usług urządzenia z sieci zewnętrznej do koniecznego minimum. W przypadku potrzeby ich dostępności, zabezpieczenie dostępu poprzez usługę VPN z wdrożonym mechanizmem uwierzytelniania wieloskładnikowego.
    - Ograniczenie dostępu do panelu zarządzania urządzeniem jedynie z dedykowanych, wewnętrznych adresów IP (whitelisting).
    - Ustawienie unikalnych, bezpiecznych haseł dla każdego urządzenia.
    - Wdrożenie wieloskładnikowego uwierzytelnienia we wszystkich usługach i serwisach, w których jest to możliwe.
3. Konfiguracja
    - Zapewnienie segmentacji sieci w oparciu o funkcje biznesowe oraz poziom krytyczności systemów oraz monitorowanie i filtrowanie ruchu sieciowego przekraczającego granicę segmentów.
    - Ograniczenie dostępu do paneli administracyjnych i krytycznych systemów z sieci zewnętrznej do koniecznego minimum. W przypadku potrzeby ich dostępności, zabezpieczenie dostępu poprzez usługę VPN z wdrożonym mechanizmem uwierzytelniania wieloskładnikowego.
    - Weryfikacja, czy hasła w pliku konfiguracyjnym urządzenia są przechowywane w sposób uniemożliwiający ich przejęcie (z wykorzystaniem bezpiecznej funkcji haszującej).
4. Monitoring
    - Cykliczna weryfikacja kont użytkowników i ich uprawnień.
    - Cykliczny monitoring alarmów generowanych przez systemy bezpieczeństwa urządzenia.
    - Weryfikacja poziomu logowania i ustawienie logowania dla ważnych zdarzeń m.in. logowania użytkowników, logowania VPN, logowania zmian w konfiguracji.
    - Zapewnienie przekierowania logów do dedykowanego urządzenia w celu ochrony przed ich utratą.
    - Regularne monitorowanie logów pod kątem wystąpienia awarii i anomalii.
    - Cykliczna weryfikacja dostępnych publicznie usług i zasobów pod kątem poprawności reguł dostępowych.
    - Regularne tworzenie kopii zapasowych konfiguracji urządzeń brzegowych oraz testowanie procedur odtwarzania po awarii.
5. Fizyczne i logiczne bezpieczeństwo

- Urządzenia brzegowe powinny znajdować się w zamkniętych, monitorowanych szafach rack w pomieszczeniach z ograniczonym dostępem.
- Zastosowanie redundantnych zasilaczy oraz systemów podtrzymywania napięcia (UPS).

Rekomendacja została opracowana w ramach współpracy Ministerstwa Cyfryzacji oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego: CSIRT NASK, CSIRT GOV, CSIRT MON.

Krzysztof Gawkowski
Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Wiceprezes Rady Ministrów
Minister Cyfryzacji

/dokument podpisany elektronicznie/

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