Wiceprezes Rady Ministrów
Minister Cyfryzacji

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Krzysztof Gawkowski

DC.WAC.5555.108.2026
Warszawa, 18 września 2026 r.

Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa
nr 2026-67-8
dotycząca bezpieczeństwa systemów OT w sektorze wodociągowo-kanalizacyjnym

Wstęp

Niniejsza rekomendacja została wydana na podstawie art. 67a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[1] (ustawa o KSC). Jej celem jest podniesienie poziomu bezpieczeństwa systemów informacyjnych i operatorskich podmiotów krajowego systemu cyberbezpieczeństwa (KSC) w związku z identyfikacją podatności w infrastrukturze w sektorze wodociągowo-kanalizacyjnym, ograniczenie ryzyka zakłócenia procesów technologicznych oraz zapewnienie ciągłości świadczenia usług wodociągowo-kanalizacyjnych.

Systemy OT[2] są często połączone z systemami IT[3] i udostępniane zdalnie pracownikom, integratorom oraz podmiotom odpowiedzialnym za ich utrzymanie. Szczególne ryzyko stanowi bezpośrednia dostępność systemów OT i ich paneli administracyjnych z sieci Internet, która może umożliwić nieuprawniony dostęp do systemów automatyki.

Rekomendacja

W celu minimalizacji ryzyka nieuprawnionego dostępu do mechanizmów zarządzania systemami OT rekomenduję:

1. Stosowanie w architekturze systemów:
   - separację urządzeń OT od sieci Internet – tak, aby dostęp do nich nie był możliwy bezpośrednio;
   - szyfrowanych kanałów dostępu do sieci z urządzeniami OT z zewnątrz sieci organizacji, np. na potrzeby zdalnego dostępu administratora lub wsparcia producenta;
   - dedykowanych sieci OT oddzielonych od sieci korporacyjnej oraz stref DMZ[4] przy użyciu aktywnych reguł na zaporze sieciowej;
   - stosowanie wersji oprogramowania zawierających najnowsze aktualizacje zabezpieczeń;
   - objęcie systemów OT mechanizmami zarządzania odtworzeniem po awarii, kopii zapasowej, w tym ich konfiguracji.
2. Stosowanie mechanizmów uwierzytelnienia i zarządzania uprawnieniami:
   - wieloskładnikowego uwierzytelniania;

[1] Dz. U. z 2026 r. poz. 20 z późn. zm.
[2] Technologia operacyjna (OT – Operational Technology).
[3] Technologie informacyjne (IT – Information Technology).
[4] Wydzielony segment sieci komputerowej, przeznaczony dla usług i ograniczający możliwość bezpośredniego dostępu do chronionych zasobów (DMZ - Demilitarized Zone).

telefon: +48 22 245 59 22
adres email: sekretariat.dc@cyfra.gov.pl
www.gov.pl/cyfryzacja

ul. Królewska 27
00-060 Warszawa

- zmianę domyślnych poświadczeń administracyjnych (login, hasło);
- wyłączenie domyślnych wbudowanych kont użytkowników;
- blokowania nieużywanych kont użytkowników;
- stosowanie indywidualnych kont użytkowników tam, gdzie jest to możliwe;
- stosowanie polityki minimalnych uprawnień.

3. Stosowanie mechanizmów audytu:
   - logowanie zdarzeń administracyjnych, zmian konfiguracji;
   - gromadzenie logów z urządzeń OT w centralnym repozytorium np. SIEM;
   - monitorowanie zdarzeń bezpieczeństwa z sieci OT;
   - cykliczny przegląd reguł dostępowych na zaporach sieciowych oraz urządzeniach dostępowych np. koncentratorach VPN;
   - cykliczny przegląd kont użytkowników oraz przypisanych uprawnień.
4. Ujęcie systemów OT w Systemie Zarządzania Bezpieczeństwem Informacji (SZBI):
   - ująć systemy w procesie testów bezpieczeństwa;
   - ująć systemy w procesie zarządzania podatnościami;
   - ująć systemy w procesie analizy ryzyka dla organizacji;
   - wdrożyć i stosować procedury wycofania urządzeń po zakończeniu wsparcia producenta.
5. Stosować się do zaleceń oraz ostrzeżeń wydawanych przez zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) oraz utrzymywać z nimi kanały komunikacji.

Rekomendacja została opracowana w ramach współpracy Ministerstwa Cyfryzacji i CSIRT Infrastruktura.

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

telefon: +48 22 245 59 22
adres email: sekretariat.dc@cyfra.gov.pl
www.gov.pl/cyfryzacja
ul. Królewska 27
00-060 Warszawa