OD AUDYTU DO CYBERODPORNOŚCI – JAK SKUTECZNIE PRZYGOTOWAĆ WODOCIĄGI NA NOWE ZAGROŻENIA

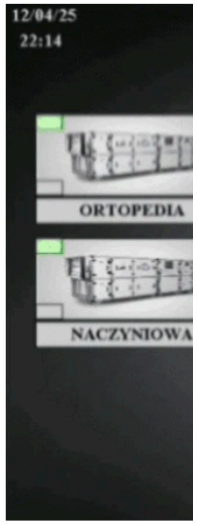
Cyberbezpieczeństwo Infrastruktury Krytycznej Wod-Kan

CYBER ARMY OF RUSSIA REBORN

Źródło: SOCRadar

Zaatakowano polski szpital i oczyszc

OSKAR KLIMCZUK
16.04.2025 07:46



Grupa prorosyjskich cyberprze
Autor. Telegram cyberprzestępc

Jedna z zaatakowanych
Autor. Telegram cyberp

Rosjanie zaatakowali polską elektrownię i wodociąg

OSKAR KLIMCZUK
01.07.2025 14:54

DRUKUJ PDF

Cyberatak w przestworzach – linie lotnicze na celowniku hakerów
Autor. CyberDefence24

Cyberataki na polskie wodociągi i oczyszczalnie są realnym zagrożeniem, co potwierdzają kolejne incydenty. Tym razem do tego grona dołączyła elektrownia wodna. Na celowniku cyberprzestępców był również m.in. bioreaktor oraz jedno z przedsiębiorstw.

Źródła: CyberDefence24, Smart water magazine

PODATNOŚCI

SharePoint pod ostrzałem hakerów

Krytyczna podatność typu zero-day w Microsoft SharePoint Server jest wykorzystywana w globalnej kampanii cyberataków

Źródło: CRN

CELE ATAKUJĄCYCH

CEL ZAROBKOWY (OKUP)

- Pozyskanie danych osobowych lub informacji wrażliwych
- Zaszyfrowanie danych w celu zatrzymania pracy

CELE ATAKUJĄCYCH

CEL GEOPOLITYCZNY

- Wywołanie chaosu
- Zastraszenie społeczeństwa
- Wzbudzenie niepokoju społecznego

SKUTKI ATAKÓW

- Straty finansowe
- Skażenie zasobów wodnych
- Przerwy w świadczeniu usług
- Utrata zaufania publicznego do systemów wod-kan

ATAKI NA WODOCIĄGI

TRENDY ATAKÓW

1. Systemy SCADA - główny cel dla hakerów, którzy chcą manipulować dystrybucją i oczyszczaniem wody
2. Urządzenia IoT obecne w przemysłowych systemach sterowania
3. Ransomware - ogólna infrastruktura IT

AUDYT

AUDYT

PO CO NAM AUDYT

Audyt jako punkt wyjścia do dalszych działań

- zakupy sprzętu i oprogramowania - inwentaryzacja obecnych rozwiązań i audyt stanu ich zabezpieczeń
- wdrożenie/aktualizacja SZBI - audyt obecnej dokumentacji
- analiza ryzyka - audyt istniejących zabezpieczeń
- zgodność z przepisami - to audyt zgodności

AUDYT - MIT

Często słyszymy: ‘Najpierw kupmy sprzęt i zróbmy wdrożenie, a potem sprawdźmy audytem, czy wszystko jest bezpieczne’.
To jeden z najgroźniejszych mitów!

Tymczasem bezpieczeństwo zaczyna się od świadomego planowania i analizy już na etapie wyboru rozwiązań

Audyt to nie kontrola po fakcie, ale narzędzie, które powinno towarzyszyć nam od początku całego procesu – od planowania po eksploatację.

CZYM JEST AUDYT ZEROWY?

W PRZEDSIĘBIORSTWACH WODNO-KANALIZACYJNYCH JEST TO

- Wstępne, kompleksowe sprawdzenie zabezpieczeń IT/OT
- Identyfikacja krytycznych systemów, procesów i przepływów danych
- Ocena gotowości organizacji na zagrożenia cybernetyczne
- Podstawa do dalszych działań naprawczych i inwestycji

ETAPY AUDYTU ZEROWEGO

1. Mapowanie infrastruktury IT/OT: Identyfikacja kluczowych systemów, analiza przepływów danych, dostępu i zabezpieczeń
2. Przegląd ryzyk: Identyfikacja zagrożeń, weryfikacja zabezpieczeń stacji uzdatniania wody, SCADA, sieci
3. Przegląd polityk i procedur: Analiza polityk bezpieczeństwa i planów reagowania na incydenty
4. Raport i rekomendacje: Szczegółowy opis stanu bezpieczeństwa, propozycje modernizacji, narzędzi i szkoleń

KORZYŚCI Z AUDYTU ZEROWEGO

- identyfikacja i przygotowanie do eliminacji słabych punktów
- zrozumienie aktualnego stanu zabezpieczeń i ryzyk
- lepsze planowanie inwestycji i rozwoju
- początek drogi do skuteczniejszej reakcji na incydenty
- wzrost odporności na cyberzagrożenia
- przygotowanie do spełnienia wymagań przepisów prawa (np. NIS2)

DLACZEGO WARTO DZIAŁAĆ TERAZ?

- Proaktywne podejście = mniejsze ryzyko strat finansowych i operacyjnych
- Punkt wyjścia do prac na dokumentacją i wewnętrznymi procedurami
- Przygotowanie do przyszłych wyzwań i regulacji
- Audyt to kluczowy element prewencji – jak kontrola jakości wody

CO PO AUDYCIE?

- wdrożenie wniosków audytowych
- analiza ryzyka

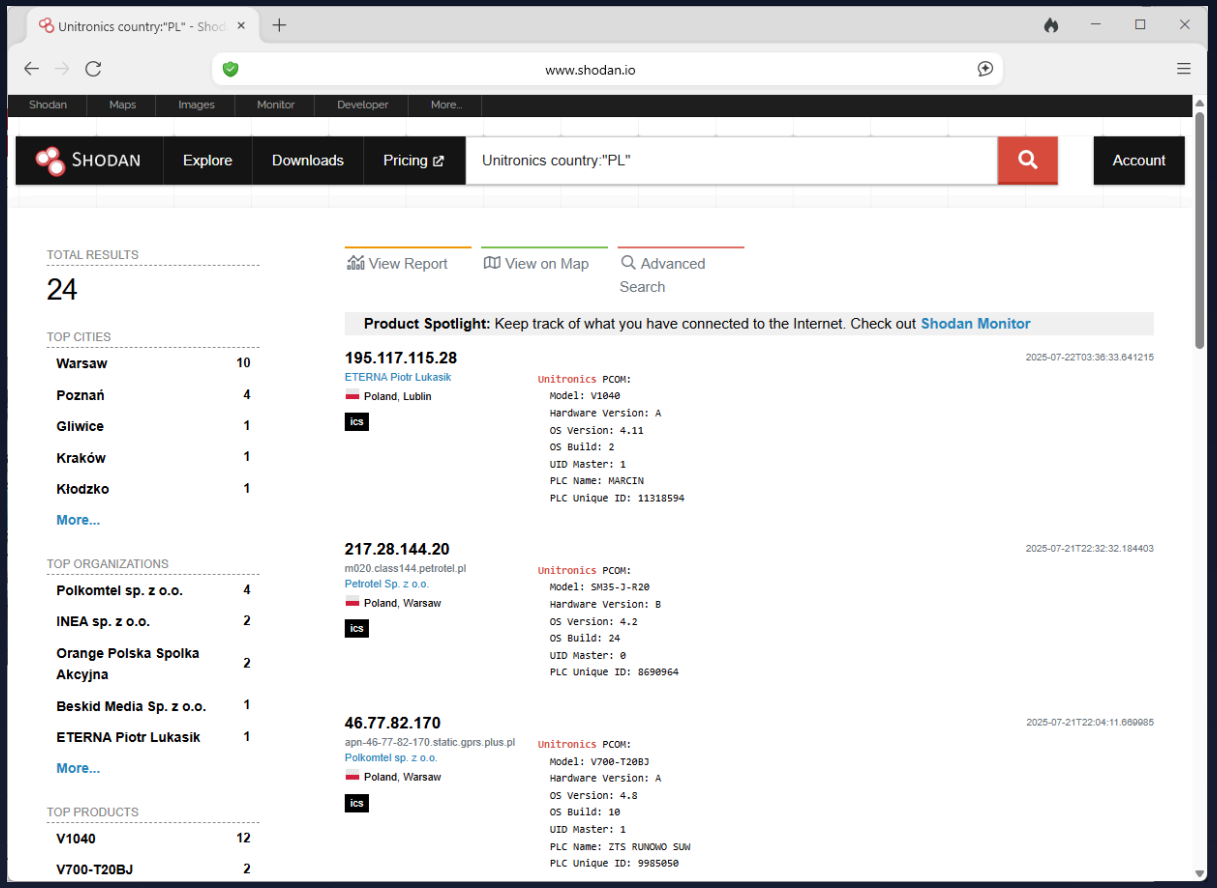
REKOMENDACJE CYBERBEZPIECZEŃSTWA

CISA, KPRM

- ogranicz ekspozycję na publiczny dostęp z Internetu
- przeprowadzaj regularne oceny cyberbezpieczeństwa
- natychmiast zmień domyślne hasła
- przeprowadź inwentaryzację zasobów technologii operacyjnej/informacyjnej
- opracuj i ćwicz plany reagowania na incydenty cyberbezpieczeństwa
- wykonaj kopię zapasową systemów
- ogranicz narażenie na podatności
- przeprowadzaj szkolenia z zakresu świadomości cyberbezpieczeństwa

https://www.gov.pl/attachment/d607b4f3-5ac7-4f1f-8688-3f42d93c6af9

EKSPOZYCJA NA PUBLICZNY DOSTĘP Z INTERNETU



Źródło: shodan.io

DZIĘKUJĘ ZA UWAGĘ

k.wagner@itaudit.pl