



**WNIOSKI Z AUDYTÓW CYBERBEZPIECZEŃSTWA  
– CZYLI JAK ZABEZPIECZYĆ INFRASTRUKTURĘ OT  
W PRZEDSIĘBIORSTWIE WOD-KAN**

XXIII Forum Wymiany Doświadczeń –  
Zielona Góra 2025

# O NAS



ICsec S.A. to **polski** producent rozwiązań z zakresu cyberbezpieczeństwa dedykowanych dla przemysłu, w tym **infrastruktury krytycznej**.



Zaprojektowaliśmy, opracowaliśmy, przetestowaliśmy i wdrażamy system **SCADvance XP** – innowacyjny system monitorowania sieci przemysłowych zapewniający identyfikację, monitoring oraz bezpieczeństwo posiadanych zasobów sieci OT w czasie rzeczywistym.



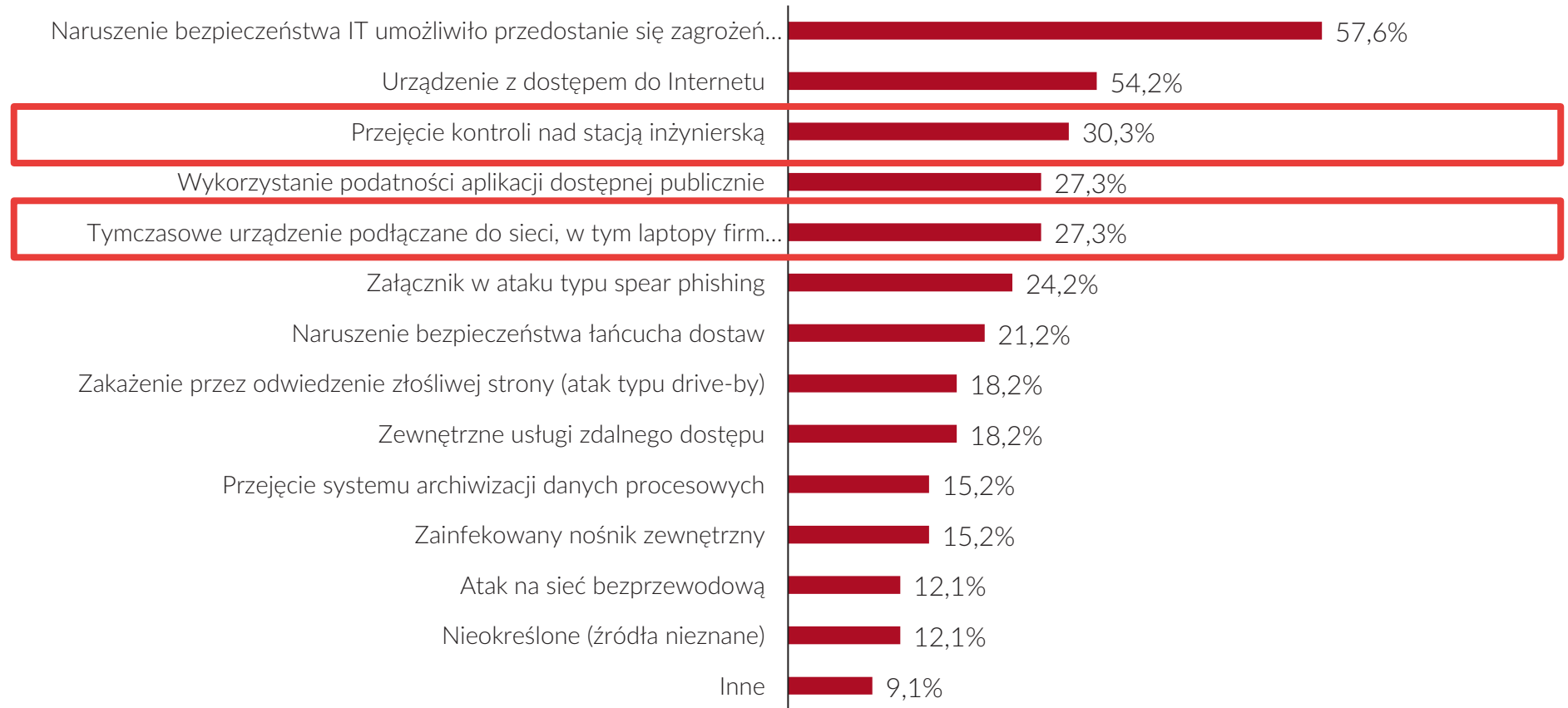
# TRENDY W CYBERBEZPIECZEŃSTWIE



# NAJCZĘSTSZE WEKTORY ATAKÓW

**Pytanie:**

Wybierz trzy najważniejsze wektory zagrożeń, które najbardziej Cię dotyczą.



# PRZYKŁADY ATAKÓW NA SEKTOR UTILITIES

## 2023 – Irlandia

- Mały wodociąg w hrabstwie Mayo
- Atakujący uzyskali dostęp do sterownika PLC odpowiedzialnego za **utrzymanie ciśnienia wody** i wyłączyli go zdalnie

## 2024 - USA

- Atak grupy Sandworm na **systemy zdalnego sterowania wodociągami** w Teksasie
- Hakerzy uzyskali zdalny dostęp do systemów SCADA/HMI
- Atakujący spowodowali **przepełnienie zbiorników wodnych**

## 2024 – Wielka Brytania (SouthernWater)

- Jeden z największych **dostawców wody i usług kanalizacyjnych** padł ofiarą ataku ransomware
- Wykradzono 750 GB wrażliwych danych
- Firma oszacowała koszty ataku na 4,5 miliona funtów

W sektorze utilities odnotowano **42%\*** wzrost w liczbie cyberataków w 2024 r.

# CZY ATAKI NA SEKTOR UTILITIES W POLSCE SĄ MOŻLIWE?

*„Wiemy, że delegowane są dwie grupy, które stworzyła rosyjska GRU [wywiad wojskowy], aby przeprowadzać cyberataki na Polskę.*

*Infrastruktura **wodno-kanalizacyjna, energetyka**, administracja rządowa i samorządowa to główne kierunki cyberataków”*

*- wicepremier i minister cyfryzacji, Krzysztof Gawkowski<sup>(1)</sup>.*

# CZY ATAKI NA SEKTOR UTILITIES W POLSCE SĄ MOŻLIWE?

W I półroczu 2024 zgłoszono **ponad 400 tys. incydentów** cyberbezpieczeństwa – **wzrost o 100% r/r.** - wicepremier i minister cyfryzacji, Krzysztof Gawkowski

Luty 2024

Atak na oczyszczalnię ścieków w Polsce

Kwiecień 2024

Próba cyberataku na oczyszczalnię ścieków na Mazurach

Wrzesień 2024

Rozbicie grupy sabotażystów planujących cyberataki na polską infrastrukturę

2024

Ataki DDoS na polskie podmioty infrastruktury krytycznej

# ROSNĄCA LICZBA INCYDENTÓW

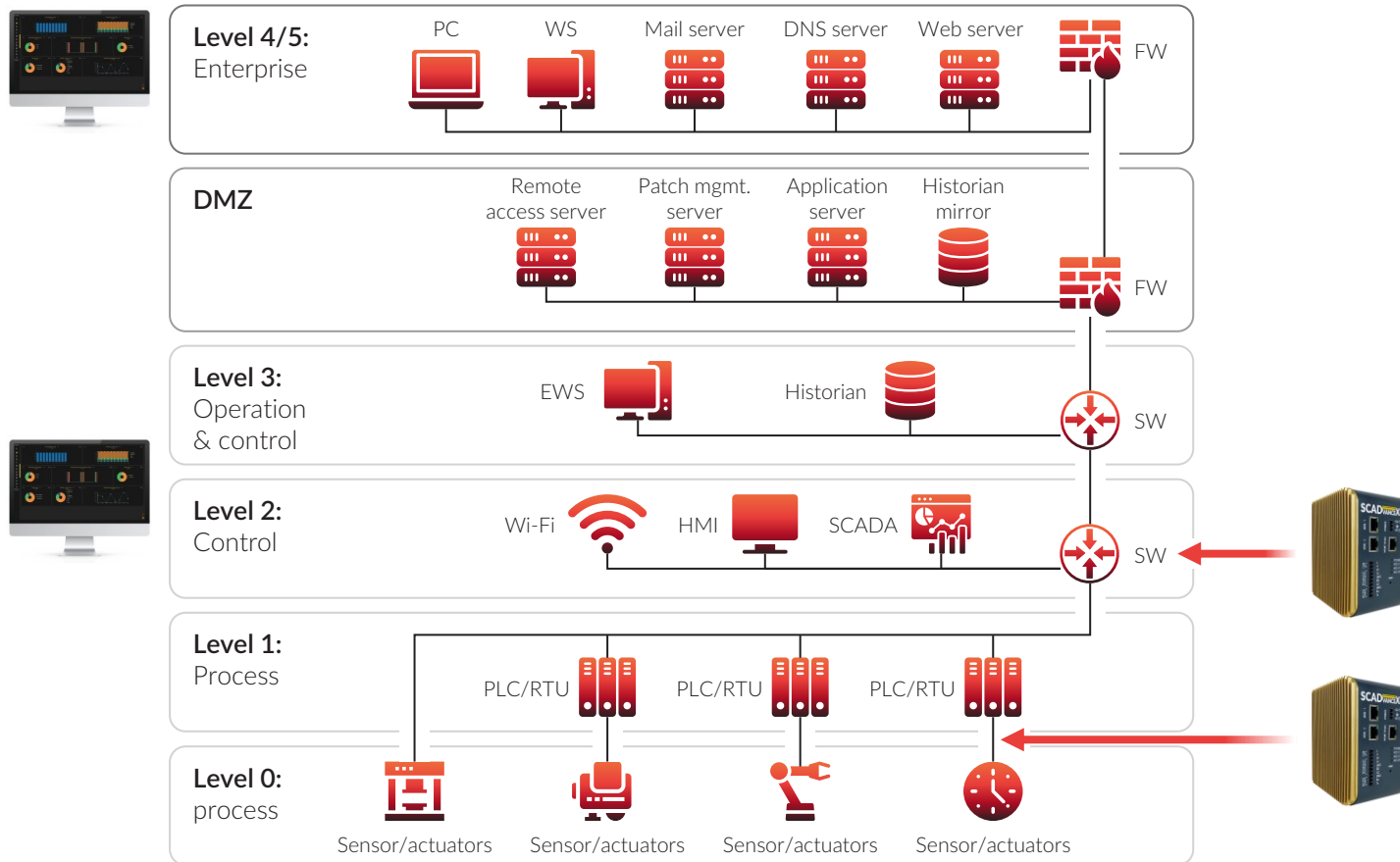
Incydenty obsłużone przez CERT Polska w latach 2019-2024 (wodociągi)	
2019r	5
2020r	9
2021r	18
2022r	9
2023r	13
2024r	59







# PRZYKŁAD ARCHITEKTURY



Operujemy w najniższych warstwach modelu PERA.

Wykorzystujemy kopię ruchu udostępnioną przez porty w przełącznikach sieciowych (SPAN/ R-SPAN port, TAP lub pass-through).

Sonda może pracować na portach szeregowych

Oprogramowanie SCADvance XP wg. preferencji klienta (domyślnie warstwa Enterprise).

System on-premise.



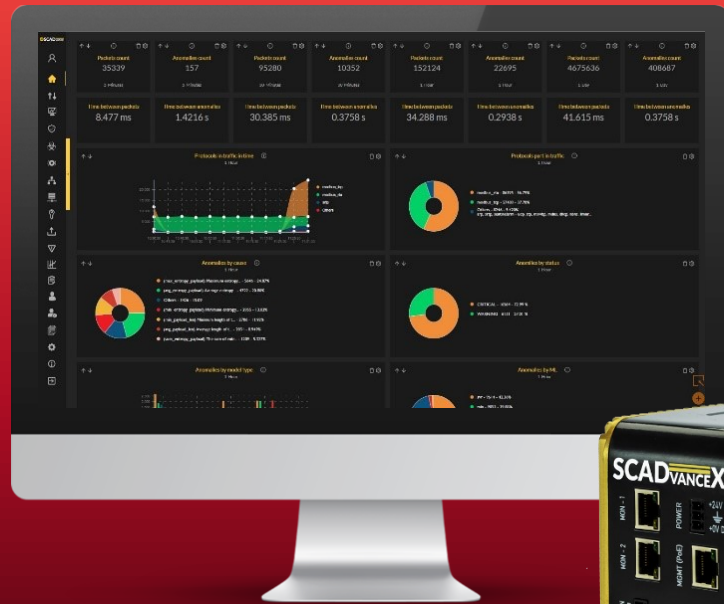
# STUDIUM CYBERATAKU

(VIDEO)



# CYBERBEZPIECZEŃSTWO DLA SIECI OT

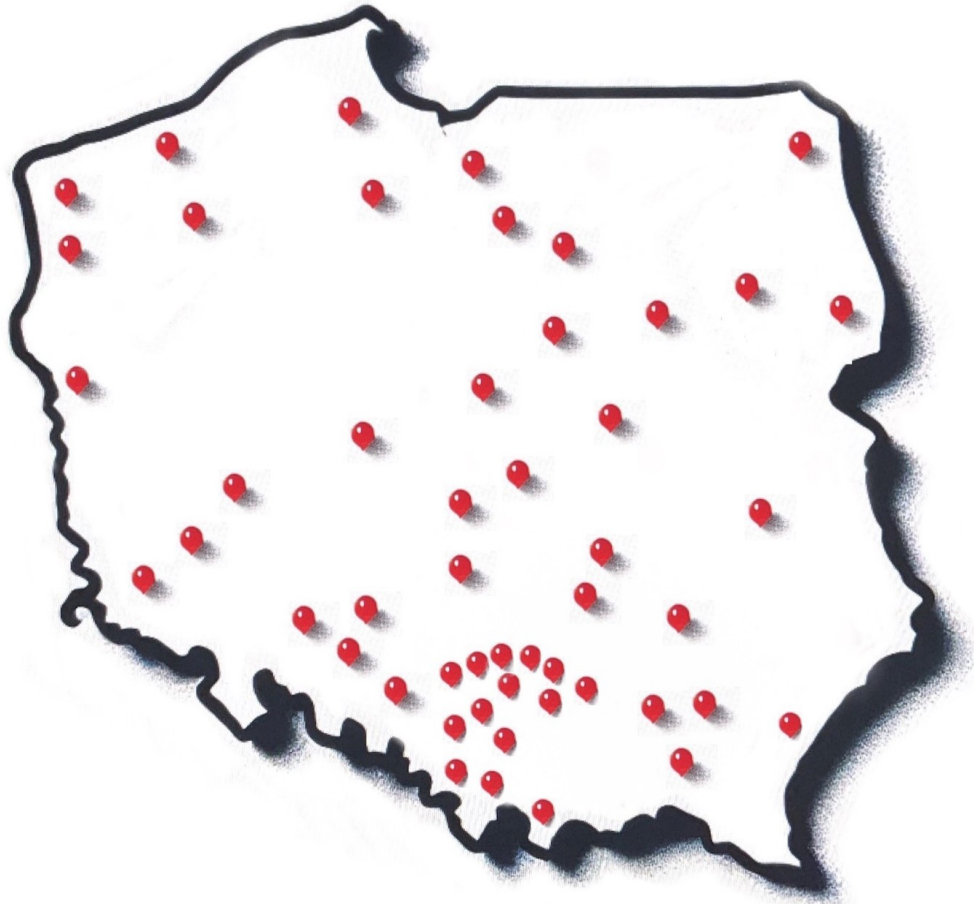
## SCADVANCEXP



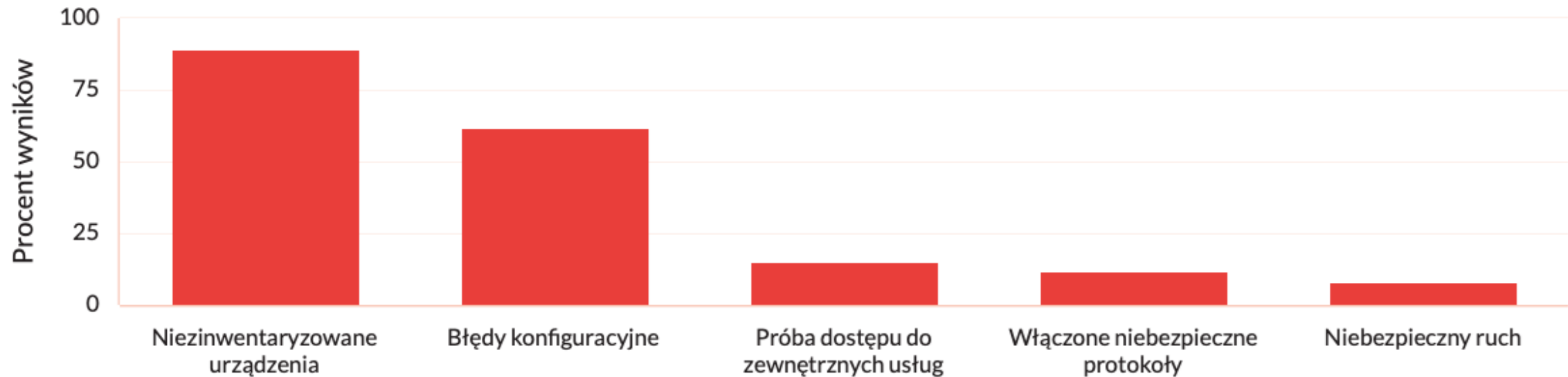
- Monitoring sieci (24/7/365)
- Inwentaryzacja
- Detekcja zagrożeń
- Statystyki i raporty
- Zarządzanie incydentami
- Zarządzanie Podatnościami

**ALE...**

# JEDYNY POLSKI PRODUCENT NA POLSKIM GRUNCIE

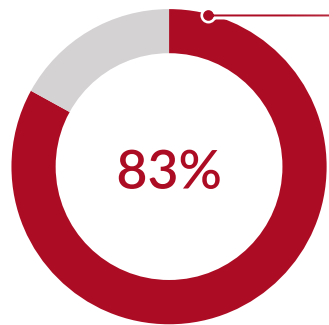


# NAJCZĘSTSZE PROBLEMY I NIEBEZPIECZEŃSTWA W SIECIACH PRZEMYSŁOWYCH



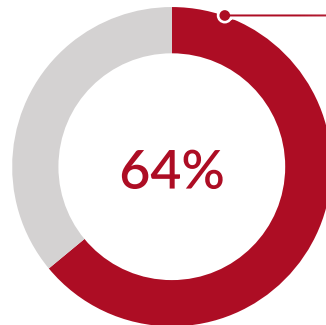
Nie ma sieci idealnej.

# WYNIKI AUDYTÓW – NAJCZĘSTSZE REALNE ZAGROŻENIA



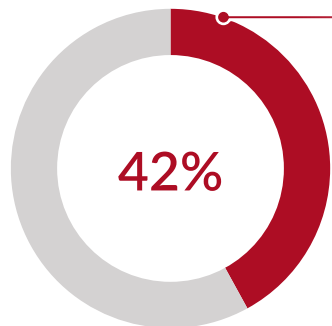
Podatności urządzeń w infrastrukturze

83%



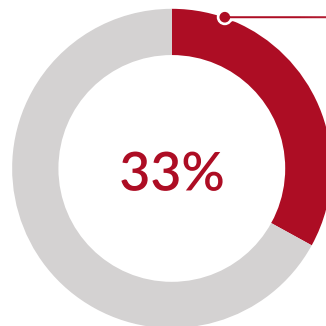
Bezpośredni dostęp do usług w Internecie

64%



Niezabezpieczony ruch SNMP

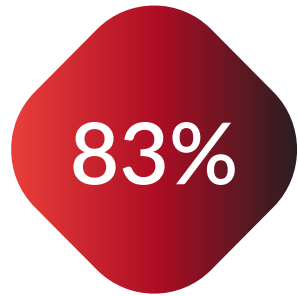
42%



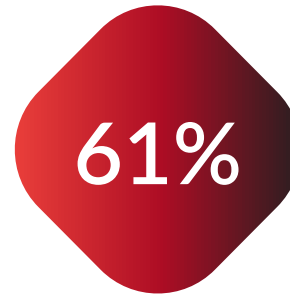
Kamery w sieci przemysłowej

33%

# WYNIKI AUDYTÓW - ZŁE PRAKTYKI



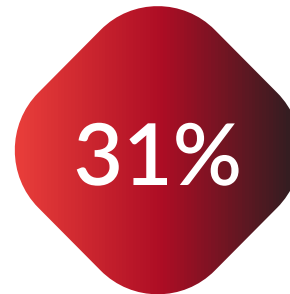
Urządzenia IPv6 w sieci  
OT



Włączony protokół UPNP  
na urządzeniach



Urządzenia z adresacją  
169.254.0.0-  
169.254.255.255



Duży ruch protokołu ICMP -  
możliwe tunelowanie



# OD CZEGO ZACZAĆ - NAJPILNIEJSZE DZIAŁANIA NAPRAWCZE



- 01 Aktualizacje urządzeń i zmiany domyślnych haseł na urządzeniach
- 02 Sieć OT nie powinna mieć możliwości bezpośredniego połączenia z siecią IT – bez wyjątków!
- 03 Stosowanie switchy zarządzanych umożliwiają zwiększenie bezpieczeństwa dostępu
- 04 Wszystkie dostępy należy realizować po przejściu przez firewall organizacji
- 05 Dostęp do infrastruktury OT filtrowany przez UTM/Firewall
- 06 Używanie adresacji RFC1918 oraz szyfrowanych wersji protokołów

# ZALECENIA

KANCELARIA PREZESA RADY MINISTRÓW

DEPARTAMENT CYBERBEZPIECZEŃSTWA

## Rekomendacje cyberbezpieczeństwa dla sektora wodno-kanalizacyjnego

(R-CYBER-01/2021)

(luty 2021 r.)

### Informacje o poradniku

Poradnik jest skierowany do specjalistów ds. bezpieczeństwa IT/OT, w szczególności, w następujących podmiotach:

- Organy właściwe ds. cyberbezpieczeństwa;
- Zespoły CSIRT poziomu krajowego;
- Operatorzy usług kluczowych;
- Operatorzy infrastruktury krytycznej;
- Urzędy administracji rządowej i samorządowej.

## Komunikat Pełnomocnika Rządu do spraw Cyberbezpieczeństwa ws. ataków na przemysłowe systemy sterowania

25.02.2025

Pełnomocnik Rządu do spraw Cyberbezpieczeństwa, Krzysztof Gawkowski, informuje o rosnącej liczbie ataków na przemysłowe systemy sterowania (ICS/OT) dostępne z internetu. Zdarzenia te są często działaniami aktywistów, a ich celem jest zwrócenie uwagi mediów na udany atak. Co ważne, niektóre z tych ataków miały wpływ na rzeczywiste działanie systemów, a ich skutki odczuli odbiorcy usług.



# Q&A



# Agnieszka Kornacka

Sales Executive, ICsec S.A.

[agnieszka.kornacka@icsec.pl](mailto:agnieszka.kornacka@icsec.pl)

517 529 464



ICsec Spółka Akcyjna

[biuro@icsec.pl](mailto:biuro@icsec.pl)  
[www.icsec.pl](http://www.icsec.pl)

