Kluczowe zalecenia Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa w sprawie ataków na przemysłowe systemy sterowania (ICS/OT):

- **Zabezpieczenie komunikacji** telemetrycznej poprzez zastosowanie Prywatnego APN
- **Monitoring i reagowanie** na incydenty w sieci IT i OT
- **Separacja i segmentacja** sieci IT i OT
- **Zablokowanie portów komunikacyjnych** protokołów przemysłowych z otwartej sieci Internet, szczególnie do konfiguracji urządzeń

Kluczowe zalecenia Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa w sprawie ataków na przemysłowe systemy sterowania (ICS/OT):

- **Zabezpieczenie i kontrola dostępu** przez VPN z wykorzystaniem wieloskładnikowego uwierzytelniania (MFA) oraz realizowanie zdalnego dostępu na żądanie z identyfikowalnym czasem, celem i źródłem.
- **Cykliczna aktualizacja urządzeń** i zmiana domyślnych danych uwierzytelniających
- **Zgłoszenie osoby kontaktowej** do odpowiedniego CSIRT-u krajowego oraz systematyczna aktualizacja kontaktu.

EXATEL

W ramach projektu „Cyberbezpieczne Wodociągi”, zakomunikowane zostały trzy główne obszary konkursu, które będą dodatkowo premiowane w ramach kosztów kwalifikowanych:

obszar kompetencji

obszar techniczny IT

obszar techniczny OT

EXATEL

I OBSZAR KOMPETENCJI:

- Szkolenia z zakresu cyberbezpieczeństwa

II OBSZAR TECHNICZNY IT:

- Rozwiązania bezpieczeństwa sieci
- Rozwiązania bezpieczeństwa styku sieci internet z usługami wewnętrznymi
- Monitorowanie bezpieczeństwa
- Zarządzanie uprawnieniami użytkowników
- Zabezpieczanie dowodów cyfrowych

EXATEL

III OBSZAR TECHNICZNY OT:

- Bezpieczeństwo systemów sterowania przemysłowego (OT/ICS/IoT)
- Bezpieczeństwo stacji roboczych OT/ICS
- Rozwiązania bezpieczeństwa sieci OT/ICS/IIoT
- Rozwiązania sieciowe WAN/LAN/Wi-Fi OT/ICS/IoT
- Rozwiązania bezpieczeństwa styku sieci internet z siecią OT/ICS/IoT
- Rozwiązania bezpieczeństwa styku sieci wewnętrznej IT z siecią OT/ICS/IoT
- Rozwiązania kopii zapasowych konfiguracji i danych systemów OT/ICS/IoT

Zgodnie z planowaną nowelizacją ustawy o Krajowym Systemie Cyberbezpieczeństwa (implementującą dyrektywę NIS-2),

przedsiębiorstwa wodociągowe świadczące usługi w zakresie zaopatrzania w wodę pitną, zostaną objęte obowiązkami jako podmioty kluczowe, niezależnie od faktu skorzystania z grantu w ramach programu **„Cyberbezpieczny Wodociąg”.**

Co to oznacza?

Że niezależnie od udziału w programie grantowym, konieczne będzie spełnienie wymagań dotyczących:

- Zarządzania ryzykiem i monitoringu podatności,
- Monitorowania i raportowania incydentów bezpieczeństwa,
  Prowadzenia audytów i testów penetracyjnych,
- Budowania świadomości pracowników w zakresie bezpieczeństwa, poprzez szkolenia i kampanie phishingowe,
- Współpracy z CSIRT.

Porozmawiajmy jak możemy Ci pomóc:

- **Paweł Sęczkowski** | +48 571 227 765 | **pawel.seczkowski@exatel.pl**
  JST Centralno-Wschodni (mazowieckie, łódzkie, lubelskie, podlaskie)

- **Robert Kurkowski** | +48 573 002 442 | **robert.kurkowski@exatel.pl**
  JST Południowo-Wschodni (śląskie, małopolskie, podkarpackie, świętokrzyskie)

- **Paulina Brzozowska** | +48 573 002 328 | **paulina.kucharska@exatel.pl**
  JST Północny (zachodniopomorskie, pomorskie, kujawsko-pomorskie, warmińsko-mazurskie)

- **Wojciech Raduchowski** | +48 573 002 404 | **wojciech.raduchowski@exatel.pl**
  JST Zachodni (wielkopolskie, lubuskie, dolnośląskie, opolskie)

EXATEL

Porozmawiajmy jak możemy Ci pomóc:

e-mail: kontakt@exatel.pl

tel.: 22 340 66 60

Skontaktuj się z nami!