WPROWADZENIE DO CYBERBEZPIECZEŃSTWA SYSTEMÓW AUTOMATYKI PRZEMYSŁOWEJ WG. IEC 62443

WPROWADZENIE DO CYBERBEZPIECZEŃSTWA SYSTEMÓW AUTOMATYKI PRZEMYSŁOWEJ

- Systemy automatyki przemysłowej
- Przykłady zagrożeń dla sieci OT
- Możliwe zagrożenia systemów OT
- Podatności systemów OT
- Koncepcja Defens in Depth
- Grupy zagrożeń
- Wymagania bezpieczeństwa dla systemów OT
- IT i OT – podobieństwa i różnice
- IT i OT – atrybuty

STANDARDY WSPIERAJĄCE SYSTEMY BEZPIECZEŃSTWA INFORMACJI

1. ISO/IEC 27001
2. ISO/IEC rodzina norm ISO 27000
3. NIST
4. IEC 62443
5. Agencja UE ds. Cyberbezpieczeństwa ENISA
6. Dyrektywa NIS2
7. Ustawa o Krajowym Systemie Cyberbezpieczeństwa

CZŁOWIEK JAKO NAJSŁABSZE OGNIWO

- Przykładowe ataki z pominięciem narzędzi cyberbezpieczeństwa
- Dlaczego najsłabszym ogniwem jest człowiek
- Kogo wybiera cyberprzestępca

NORMA IEC 62443

- IEC 62443 – historia i struktura
- Komponenty, systemy, organizacje
- IEC 62443 – wymagania
- Ryzyko dla OT
- Szacowanie ryzyka dla OT – metodologia
- Przykłady podziału na strefy i połączenia
- Security Level – poziomy
- Wymagania dla Security Level
- Cykl życia systemów OT
- System Cyberbezpieczeństwa dla OT zgodnie z IEC62443

ROZWIĄZANIA ORGANIZACYJNE WPIERAJĄCE CYBERBEZPIECZEŃSTWO OT

- System bezpieczeństwa
- Postępowanie z komputerami
- Zarządzania zmianami i kopiami zapasowymi
- Zarządzanie dostępem do systemu sterowania
- Zarządzanie użytkownikami
- Świadomość, role i odpowiedzialność
- Procesy bezpieczeństwa
- Audyty i testy systemu

ROZWIĄZANIA TECHNICZNE

- Monitorowanie infrastruktury sieciowej
- Zapora sieciowa
- DPI
- Bramka jednokierunkowa
- Zdalny dostęp
- Intrusion Detection System – IDS
- Intrusion Prevention System – IPS
- UTM
- SIEM