

## Spis treści

### I Bezpieczeństwo systemów automatyki przemysłowej - wprowadzenie (wersja 2003)

- I-3 Systemy automatyki w przeszłości
- I-4 Systemy automatyki dziś
- I-5 Motywacja i trendy rozwoju systemów automatyki
- I-6 Wybrane konsekwencje rozwoju systemów automatyki
- I-7 Trendy zwiększające podatność systemów OT na zagrożenia
- I-8 Przykłady incydentów jakie dotknęły systemy OT – Stuxnet 2010
- I-9 Przykłady incydentów jakie dotknęły systemy OT – Industroyer 2016
- I-10 Przykłady incydentów jakie dotknęły systemy OT – Triton/Trisis 2017
- I-11 Przykłady incydentów jakie dotknęły systemy OT – NotPetya 2017
- I-12 Ostrożności nigdy za wiele ...
- I-13 ... ponieważ jej brak może sporo kosztować!
- I-14 ... a wiadomości ze świata to potwierdzają!
- I-15 Ransomware – sposoby zabezpieczenia, ograniczenia szkód
- I-16 Zgłoszone incydenty – statystyki
- I-17 Zgłoszone incydenty – statystyki
- I-18 Zgłoszone incydenty – statystyki
- I-19 Możliwe wektory ataku na systemy automatyki
- I-20 Możliwe wektory ataku na systemy automatyki - podsumowanie
- I-21 Zagrożenia dla systemów automatyki
- I-22 Typowe podatności spotykane w systemach automatyki
- I-23 Typowe sytuacje występujące w systemach automatyki zwiększające zagrożenie
- I-24 Ankieta 1 - organizacja
- I-25 Wektory ataku klasyfikacja - przykład
- I-26 Przykładowe źródła informacji o podatnościach
- I-27 CVE - opis znanej/wykrytej podatności
- I-28 CVSS – Common Vulnerability Scoring System
- I-29 Przykłady wykrytych podatności w przemysłowych systemach sterowania
- I-30 Więcej informacji w zakresie podatności
- I-31 Gotowe narzędzia pozwalające na testowanie odporności systemu ...
- I-32 ... oraz przejęcie systemu
- I-33 Jak zwiększyć poziom bezpieczeństwa systemu
- I-34 Zabezpieczenie obwodowe
- I-35 Koncepcja *Defense in Depth*
- I-36 Koncepcja *Defense in Depth*
- I-37 Koncepcja „Defense in depth”
- I-38 Grupy intruzów z jakimi należy się zmierzyć
- I-39 Wymagania pod kątem bezpieczeństwa wobec systemów
- I-40 IT, a OT – podobieństwa i różnice
- I-41 IT, a OT – priorytety

## **II Standardy, wymogi i wsparcie związane z systemami bezpieczeństwa informacji (wersja 2003)**

- II-3 ISO / IEC 27001
- II-4 ISO / IEC 27001 – standardy powiązane
- II-5 PN-ISO/IEC 27001 – implementacja
- II-6 NIST Cybersecurity Framework
- II-7 NIST Cybersecurity Framework - rdzeń
- II-8 NIST Cybersecurity Framework – poziomy implementacji
- II-9 IEC 62443
- II-10 Ustawa o Krajowym Systemie Cyberbezpieczeństwa
- II-11 Ustawa o krajowym systemie cyberbezpieczeństwa - zasięg
- II-12 Ustawa o krajowym systemie cyberbezpieczeństwa – obowiązki OUK
- II-13 Ustawa o krajowym systemie cyberbezpieczeństwa – obowiązki OUK
- II-14 Ustawa o krajowym systemie cyberbezpieczeństwa – obowiązki DUC
- II-15 Ustawa o krajowym systemie cyberbezpieczeństwa – obowiązki DUC
- II-16 Normy i dobre praktyki wspomagające wdrożenie ustawy o KSC
- II-17 Agencja EU ds. Cyberbezpieczeństwa ENISA

## **III Standard IEC 62446 - wprowadzenie (wersja 2003)**

- III-3 IEC 62443 - historia
- III-4 IEC 62443 - struktura
- III-5 Standard IEC 62443 - struktura
- III-6 IEC 62443-1 – specyfikacje grupy *General*
- III-7 IEC 62443-1 – specyfikacje grupy *Policies&Procedures*
- III-8 IEC 62443-1 – specyfikacje grupy *System*
- III-9 IEC 62443-1 – specyfikacje grupy *Component*
- III-10 Główne części IEC 62443 oraz ich odbiorcy
- III-11 Certyfikacja produktów zgodnie z wymogami IEC 62443-4
- III-12 Certyfikacja produktów – certyfikowane komponenty
- III-13 Certyfikacja produktów – certyfikowane systemy
- III-14 Certyfikacja produktów – certyfikowane organizacje
- III-15 Wymagania podstawowe
- III-16 Koncepcja „Defense in depth”
- III-17 „Defense in depth” – przykładowe zabezpieczenia
- III-18 Zakres ochrony – zasoby oraz ich wartościowanie
- III-19 Ryzyko
- III-20 Ryzyko - przykłady
- III-21 Zagrożenia
- III-22 Zagrożenia o charakterze aktywnym - przykłady
- III-23 Zagrożenia o charakterze aktywnym – przykłady cd.
- III-24 Podatność
- III-25 Ankieta 2 - podatności
- III-26 Proces oceny ryzyka
- III-27 Podejście do minimalizowania ryzyka
- III-28 Reakcja na zdefiniowane ryzyka
- III-29 Przeciwdziałania
- III-30 Przeciwdziałania – przykłady
- III-31 Przeciwdziałania – przykłady cd.
- III-32 Poprawa bezpieczeństwa cybernetycznego systemu - porównanie
- III-33 Dojrzałość systemu przeciwdziałania zagrożeniom cybernetycznym
- III-34 Poziom bezpieczeństwa cybernetycznego w czasie
- III-35 Szkolenia jako element systemu bezpieczeństwa
- III-36 Cykl życia systemu bezpieczeństwa
- III-37 Cykl życia systemu bezpieczeństwa cd.
- III-38 Sposoby postępowania: polityka bezpieczeństwa i procedury
- III-39 Polityka bezpieczeństwa i procedury – cykl życia
- III-40 Polityka i procedury bezpieczeństwa jako dokumenty operacyjne
- III-41 Typowe tematy obejmowane przez politykę i procedury bezpieczeństwa
- III-42 Typowe tematy obejmowane przez politykę i procedury bezpieczeństwa cd.
- III-43 Architektura systemu

- III-44 Kryteria podziału na strefy i połączenia
- III-45 Podział na strefy i połączenia - przykład
- III-46 Poziom bezpieczeństwa - koncepcja
- III-47 Poziom bezpieczeństwa (*Security Level*)
- III-48 Poziom bezpieczeństwa - typy
- III-49 SL-T - docelowy poziom bezpieczeństwa
- III-50 SL-A - osiągnięty poziom bezpieczeństwa
- III-51 SL-C - osiągalny poziom bezpieczeństwa
- III-52 Poziom bezpieczeństwa, a wymagania jakie należy spełnić
- III-53 Wymagania dla SL – przykłady
- III-54 Cykl życia Systemu Zarządzania Cyberbezpieczeństwem według IEC 62443
- III-55 Cykl życia Systemu Zarządzania Cyberbezpieczeństwem według IEC 62443 cd.
- III-56 System Zarządzania Cyberbezpieczeństwem
- III-57 Proces opracowywania Systemu Zarządzania Cyberbezpieczeństwem
- III-58 Model sieci używany w standardach IEC 62443
- III-59 Model systemu SCADA używany w standardach IEC 62443
- III-60 Architektura referencyjna
- III-61 Podział na strefy i połączenia
- III-62 Podział na strefy - przykłady
- III-63 Charakterystyka stref
- III-64 Definicja połączeń
- III-65 Charakterystyka połączeń
- III-66 Cykl życia Systemu Zarządzania Cyberbezpieczeństwem według IEC

#### **IV Rozwiązania techniczne wspierające cyberbezpieczeństwo (wersja 2003)**

- IV-3 Monitorowanie infrastruktury sieciowej
- IV-4 Bezpieczny zdalny dostęp
- IV-5 Dioda danych
- IV-6 Zapora (*Firewall*)
- IV-7 Deep Packet Inspection (DPI)
- IV-8 Intrusion Detection System (IDS)
- IV-9 IDS – detekcja bazująca na sygnaturach
- IV-10 IDS – detekcja anomalii
- IV-11 Korzyści wynikające ze stosowania systemu IDS
- IV-12 Intrusion Prevention System (IPS)
- IV-13 Zapory kolejnej generacji - *Next Generation Firewall, Unified Threat Management*
- IV-14 Security Information and Event Management (SIEM)

#### **V Rozwiązania organizacyjne wspierające cyberbezpieczeństwo (wersja 2003)**

- V-3 Postępowanie z komputerami
- V-4 Zarządzanie zmianami i kopiami zapasowymi
- V-5 Dostęp do systemu sterowania
- V-6 Wybór dostawcy systemu/przejęcie systemu w użytkowanie
- V-7 Zarządzanie użytkownikami systemu
- V-8 Świadomość, odpowiedzialność i kompetencje personelu
- V-9 Polityka bezpieczeństwa
- V-10 Procedury bezpieczeństwa
- V-11 Audyty wewnętrzne, zewnętrzne i testy

#### **VI Bezpieczeństwo systemów automatyki przemysłowej - podsumowanie (wersja 2003)**

- VI-3 Functional Safety, a Security
- VI-4 Zakup cyberbezpieczeństwa
- VI-5 Monitorowanie systemu
- VI-6 Kontekst i wsparcie
- VI-7 Świadomość
- VI-8 Wsparcie INTEX - szkolenia
- VI-9 Wsparcie INTEX - audyty