

Spis treści

I Bezpieczeństwo systemów automatyki przemysłowej - wprowadzenie (wersja 2009)

- 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 Przykładowe źródła informacji o podatnościach
- I-25 CVE - opis znanej/wykrytej podatności
- I-26 CVSS – Common Vulnerability Scoring System
- I-27 Przykłady wykrytych podatności w przemysłowych systemach sterowania
- I-28 Więcej informacji w zakresie podatności
- I-29 Gotowe narzędzia pozwalające na testowanie odporności systemu ...
- I-30 ... oraz przejęcie systemu
- I-31 Jak zwiększyć poziom bezpieczeństwa systemu
- I-32 Zabezpieczenie obwodowe
- I-33 Koncepcja *Defense in Depth*
- I-34 Koncepcja *Defense in Depth*
- I-35 Koncepcja „Defense in depth”
- I-36 Grupy intruzów z jakimi należy się zmierzyć
- I-37 Wymagania pod kątem bezpieczeństwa wobec systemów
- I-38 IT, a OT – podobieństwa i różnice
- I-39 IT, a OT – priorytety
- I-40 Systemy OT: zabezpieczenia - typowa sytuacja

II Standardy, wymogi i wsparcie związane z systemami bezpieczeństwa informacji (wersja 2007)

- II-3 ISO / IEC 27001
- II-4 ISO / IEC 27001
- II-5 ISO / IEC 27001 – standardy powiązane
- II-6 PN-ISO/IEC 27001 – implementacja
- II-7 NIST Cybersecurity Framework
- II-8 NIST Cybersecurity Framework - rdzeń
- II-9 NIST Cybersecurity Framework – poziomy implementacji
- II-10 IEC 62443
- II-11 Ustawa o Krajowym Systemie Cyberbezpieczeństwa
- 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 Agencja EU ds. Cyberbezpieczeństwa ENISA

III Standard IEC 62443 – wprowadzenie (wersja 2009)

- 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 62443-2 – specyfikacje grupy *Policies&Procedures*
- III-8 IEC 62443-3 – specyfikacje grupy *System*
- III-9 IEC 62443-4 – 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 Zakres ochrony – zasoby oraz ich wartościowanie
- III-18 Ryzyko
- III-19 Ryzyko - przykłady
- III-20 Zagrożenia
- III-21 Zagrożenia o charakterze aktywnym - przykłady
- III-22 Zagrożenia o charakterze aktywnym – przykłady cd.
- III-23 Podatność
- III-24 Proces oceny ryzyka
- III-25 Podejście do minimalizowania ryzyka
- III-26 Reakcja na zdefiniowane ryzyka
- III-27 Przeciwdziałania
- III-28 Przeciwdziałania – przykłady
- III-29 Przeciwdziałania – przykłady cd.
- III-30 Dojrzałość systemu przeciwdziałania zagrożeniom cybernetycznym
- III-31 Szkolenia jako element systemu bezpieczeństwa
- III-32 Cykl życia systemu bezpieczeństwa
- III-33 Cykl życia systemu bezpieczeństwa cd.
- III-34 Poziom bezpieczeństwa cybernetycznego w czasie
- III-35 Sposoby postępowania: polityka bezpieczeństwa i procedury
- III-36 Polityka bezpieczeństwa i procedury – cykl życia
- III-37 Architektura systemu
- III-38 Proces opracowywania Systemu Zarządzania Cyberbezpieczeństwem
- III-39 Kryteria podziału na strefy i połączenia
- III-40 Poziom bezpieczeństwa - koncepcja
- III-41 Podział na strefy i połączenia - przykład
- III-42 Architektura referencyjna
- III-43 Model sieci używany w standardach IEC 62443
- III-44 Model systemu SCADA używany w standardach IEC 62443
- III-45 Podział na strefy i połączenia
- III-46 Charakterystyka stref
- III-47 Definicja połączeń
- III-48 Charakterystyka połączeń
- III-49 Poziom bezpieczeństwa (*Security Level*)
- III-50 Poziom bezpieczeństwa - typy
- III-51 SL-T - docelowy poziom bezpieczeństwa
- III-52 SL-A - osiągnięty poziom bezpieczeństwa
- III-53 SL-C - osiągalny poziom bezpieczeństwa
- III-54 Poziom bezpieczeństwa, a wymagania jakie należy spełnić
- III-55 Wymagania dla SL – przykłady
- III-56 Cykl życia Systemu Zarządzania Cyberbezpieczeństwem według IEC 62443
- III-57 Cykl życia Systemu Zarządzania Cyberbezpieczeństwem według IEC 62443 cd.
- III-58 System Zarządzania Cyberbezpieczeństwem

IV Rozwiązania organizacyjne wspierające cyberbezpieczeństwo (wersja 2007)

- IV-3 Optymalny zestaw zapewniający bezpieczeństwo
- IV-4 Postępowanie z komputerami
- IV-5 Zarządzanie zmianami i kopiami zapasowymi
- IV-6 Dostęp do systemu sterowania
- IV-7 Wybór dostawcy systemu/przejęcie systemu w użytkowanie
- IV-8 Zarządzanie użytkownikami systemu
- IV-9 Świadomość, odpowiedzialność i kompetencje personelu
- IV-10 Polityka bezpieczeństwa
- IV-11 Procedury bezpieczeństwa
- IV-12 Audyty wewnętrzne, zewnętrzne i testy

V Rozwiązania techniczne wspierające cyberbezpieczeństwo (wersja 2009)

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

