Cyber bezpieczeństwo systemów **OT**

Systemy automatyki

Twoje IT
jest już odpowiednio zabezpieczone.
To bardzo dobrze.

A Twoje OT?
Czy ono także jest bezpieczne?

IEC 62443

Zabezpieczymy Twój system OT na dziś i na przyszłość

Oferujemy pomoc i wsparcie od oceny automatyzacji i infrastruktury OT, poprzez ocenę własnych ryzyk, planowanie konkretnych działań i ustalenie celów aż po wdrożenie i kontrolę.

1. Audyt bezpieczeństwa w warstwie procesowo-organizacyjnej w obszarze OT w oparciu o wybrany standard cyberbezpieczeństwa
2. Inwentaryzacja i ocena bezpieczeństwa elementów w wybranych/ kluczowych instalacjach OT
3. Realizacja analizy konfiguracji bezpieczeństwa wybranej próbki urządzeń OT dla kluczowych instalacji OT
4. Opracowanie rekomendacji dalszych działań mających na celu podniesienie poziomu cyberbezpieczeństwa OT
5. Realizacja zapisów rekomendacji:
   - Dostarczenie rozwiązań (software, hardware)
   - Zalecenia konfiguracji/ konfiguracja urządzeń i systemu zarządzania OT
6. Nadzór nad wdrożeniem
7. Testowanie rozwiązania w środowisku preprodukcyjnym
8. Nadzór nad eksploatacją:
   - Dostarczanie aktualizacji
   - Serwis/ umowa serwisowa
   - Monitoring ruchu w sieci
   - Analiza zdarzeń

8 Kroków do cyber bezpieczeństwa

System IDS

BEZPIECZEŃSTWO OPROGRAMOWANIA

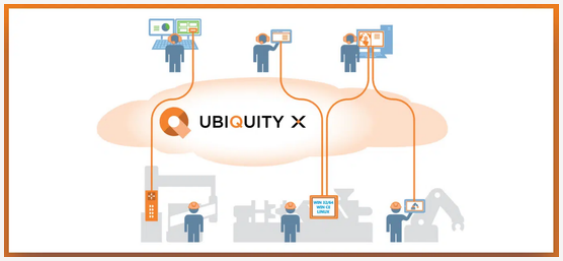
PcVue

- Bezpieczny pakiet instalacyjny
- Uwierzytelnianie i integralność
- Bezpieczne pobieranie
- Szyfrowanie pliku konfiguracyjnego
- Zaawansowane uprawnienia użytkownika
- Integracja z Active Directory
- Przemysłowe zapory sieciowe/VPN

supervisor Saia PCD®

- Uwierzytelnianie użytkowników
- Szyfrowanie danych
- Zarządzanie rolami i uprawnieniami
- Rejestracja zdarzeń w dzienniku audytu

BEZPIECZNY ZDALNY DOSTĘP



- Przemysłowe, bezpieczne połączenie VPN
- Protokoły SSL/TLS
- Szyfrowanie asymetryczne
- Certyfikat X509
- Zarządzanie użytkownikami
- Autoryzacja połączeń
- Uwierzytelnienie, także dwuskładnikowe
- Polityka haseł
- Certyfikat zgodności IEC 62443-3-3 i 62443-4-2

BEZPIECZNY SYSTEM STEROWANIA

Saia PCD QronoX

- Certyfikat zgodności z normą IEC 62443, SL3+
- Bezpieczny Webserver (HTTPS)
- Wbudowany Firewall
- Redundancja
- System operacyjny czasu rzeczywistego QNX
- Zarządzanie użytkownikami
- Szyfrowane protokoły, np. OPC UA

Optimizer Advanced Controller

- Certyfikat zgodności z IEC 62443 na poziomie projektu i produktu
- Freamwork Niagara
- Obsługa protokołów szyfrowanych
- Opcje separacji sieci komunikacyjnych
- Szyfrowanie danych
- Autoryzacja, uwierzytelnienie

BEZPIECZNA KOMUNIKACJA

M!DGE i RipEX

- Kontrola dostępu oparta na rolach
- RADIUS, VLAN, Firewall L2, L3, L4, NAT
- Szyfrowanie AES-256-CCM (tylko dla RipEX)
- Ipsec, OpenVPN
- Syslog, SNMP, SMS
- FW z podpisem cyfrowym
- Wykrywanie sabotażu sprzętowego – HW Tamper
- Definiowanie użytkowników opartE na rolach
- Ograniczenie dostępu do tylko używanych interfejsów fizycznych i logicznych
- Zdalny dostęp szyfrowany QSSH
- Aktualizacja FW

HIDRA SWITCH

- Obsługa protokołów IEEE 802.3/802.3u/802.3x
- Redundancja sieci przez pierścień ERPS (ITU-T G.8032), RSTP, STP, kompatybilność z pierścieniem MRP (klient)
- Certyfikaty: CE, UL, NEMA, Atex strefa 2, stopień ochrony IP67
- Segmentacja sieci VLAN
- Zgodność ze standardem IEC 62443
- Zaawansowane zarządzanie warstwy 2 i warstwy 3

Kontakt

SABUR Systemy automatyki

SABUR Sp. o.o.
ul. Puławska 303
02-785 Warszawa

+48 22 549 43 53
sabur@sabur.com.pl
www.sabur.com.pl