

Warszawa 28 lutego 2020

Obszar Informatyki PKN ORLEN SA

PKN ORLEN SA



Podstawowe wymagania cyberbezpieczeństwa dla systemów automatyki ICS - OT

Dla nowobudowanych instalacji i procesu modernizacji
systemów automatyki ICS - OT

Artur Sidorko

Dokument ten definiuje minimalne wymagania cyberbezpieczeństwa, które muszą być spełnione podczas planowania, procesu zakupowego, modernizacji i wdrożenia systemu ICS

Jakiegokolwiek zmiany w poniższych wymaganiach muszą być zaakceptowane przez Dział Bezpieczeństwa IT.

Termin "ICS" (skrót ICS oznacza przemysłowe systemy sterowania min. systemy monitorowania, zabezpieczania i kontroli przemysłowej) należy interpretować w rozumieniu systemów monitorowania, sterowania i bezpieczeństwa infrastruktury przemysłowej (wszystkie stacje PC, serwery, sterowniki PLC, kontrolery, urządzenia sieciowe, specjalistyczne oprogramowanie urządzeń).

I. Wymagania Ogólne

1. Wykonawca musi zaprojektować i wdrożyć środki w celu zapewnienia dostępności, integralności, poufności systemu ICS:
 - a. dostęp do systemu ICS, tylko uprawniony i autoryzowany,
 - b. ochrona przed złośliwym oprogramowaniem,
 - c. aktualizacja oprogramowania, system operacyjny i oprogramowanie aplikacyjne zgodnie z zaleceniami dostawców.
2. Podczas fazy projektowania wszystkie rozwiązania ICS w zakresie cyberbezpieczeństwa muszą być uzgodnione z Działem Bezpieczeństwa IT PKN ORLEN.
3. Architektura rozwiązania powinna zapewnić uniknięcie pojedynczego punktu awarii, w szczególności infrastruktury i aplikacji na poziomie wymaganym przez Komórki Biznesowe i pozytywnie zaakceptowana przez Obszar Cyberbezpieczeństwa IT PKN ORLEN (na przykład: stacje operatorskie, serwery, urządzenia sieciowe zasilacze).
4. Dedykowana infrastruktura cyberbezpieczeństwu musi zostać uzgodniona z obszarem informatyki i zaakceptowana przez Dział Bezpieczeństwa IT PKN ORLEN, biorąc pod uwagę, że preferowanym rozwiązaniem jest środowisko wirtualne.
5. Dostawca zapewni w okresie gwarancyjnym usługi wsparcia dla wszystkich wdrożonych rozwiązań cybernetyczności - w odniesieniu do zasad cyberbezpieczeństwa IT obowiązujących na obszarze OT.
6. Obszar Cyberbezpieczeństwa IT PKN ORLEN jest uprawniony dokonać przeglądu bezpieczeństwa rozwiązań wdrożonych przez Wykonawcę między innymi:
 - a. skanowanie podatności,
 - b. weryfikację ruchu sieciowego,
 - c. weryfikację konfiguracji,
 - d. weryfikacja zainstalowanych rozwiązań.

Wykonawca jest zobowiązany do usunięcia niezgodności i zagrożeń wykrytych podczas przeprowadzonego przeglądu bezpieczeństwa.

II. Wymagania Techniczne

1. Wykonawca zobligowany jest wdrożyć system cyberbezpieczeństwa oparty o zasadę wielowarstwowego cyberbezpieczeństwa oraz wykonać wszelkie prace, które zapewnią:
 - a. Hardening komponentów ICS (serwery, stacje, urządzenia sieciowe) w szczególności:
 - każdy dostęp (fizyczny / logiczny) do portów I / O (np. USB), stacji dyskiety, CD / DVD musi być ograniczony. Dostęp może być zrealizowany jedynie dla administratorów, inni użytkownicy nie mogą posiadać dostępu do wskazanych portów.
 - należy zdefiniować i wdrożyć odpowiednie zasady (konfigurację) bezpieczeństwa cybernetycznego.
 - należy uruchomić i skonfigurować firewall-e dostępne z poziomu systemu operacyjnego (np. Windows firewall-e) tak aby włączone były jedynie usługi i porty które są wykorzystywane w trakcie eksploatacji systemu ICS oraz cyberbezpieczeństwa.
 - nieużywane aplikacje muszą być odinstalowane,
 - niewykorzystane usługi muszą być wyłączone,
 - nieużywane porty muszą być zamknięte,
 - nieużywane konta powinny zostać zablokowane lub usunięte.
 - b. Zarządzanie poprawkami systemu operacyjnego szczególnie:
 - systemy operacyjne oraz aplikacje muszą być dostarczone, wdrożone i produkcyjnie uruchomione w najnowszej stabilnej wersji wraz z ostatnią wersją poprawek zalecanych przez producenta systemu ICS,
 - mechanizm zapewniający monitorowanie, zapewnianie i dystrybuowanie poprawek systemu operacyjnego zalecanych przez producenta systemu ICS musi być dostarczony, zainstalowany i produkcyjnie uruchomiony.
 - zapewnienie dostępu do najnowszych zatwierdzonych poprawek systemu operacyjnego (preferowane rozwiązanie) / zalecanych przez producenta ICS w okresie gwarancyjnym.
 - zapewnienie bezpiecznego automatycznego mechanizmu uzyskiwania aktualizacji / poprawek do systemu operacyjnego zalecanego przez producenta ICS. Zapewnienie mechanizmów automatycznej dystrybucji dostępnych aktualizacji/poprawek systemu operacyjnego zalecanych przez producenta ICS. Każdy proces aktualizacji powinien być potwierdzony i wykonany lub nadzorowany przez administratorów odpowiedzialnych za dany system ICS.
 - Zapewnienie centralnej konsoli zarządzania, która monitoruje aktualizacje/poprawki na wszystkich stacjach komputerowych i serwerach ICS.
 - System zarządzania aktualizacjami/poprawkami dla systemu operacyjnego serwerów i stacji operatorskich,
 - System zarządzania aktualizacjami/poprawkami musi być zgodny ze wszystkimi zaleceniami producenta ICS,
 - Instrukcje dotyczące systemu zarządzania aktualizacjami/poprawkami w systemie ICS
 - c. Ochrona systemu antywirusowego z automatycznie aktualizowaną bazą szczepionek (zwalidowane sygnatury) w szczególności:
 - System antywirusowy (preferowane rozwiązanie Symantec) musi być dostarczony, zainstalowany i produkcyjnie uruchomiony na wszystkich stacjach komputerowych i

- serwerach ICS z najnowszymi zalecanymi / zatwierdzonymi sygnaturami antywirusowymi przez producenta ICS.
- Zapewnienie dostępu do najnowszych sygnatur antywirusowych zalecanych przez producenta ICS w okresie gwarancji.
 - Zapewnienie automatycznego mechanizmu pozyskiwania sygnatur antywirusowych zalecanych przez producenta ICS.
 - Zapewnienie mechanizmów automatycznej dystrybucji dostępnych sygnatur antywirusowych zalecanych przez producenta ICS.
 - Jeśli to możliwe, wszystkie stacje komputerowe (operator, inżynieria itp.) Muszą mieć zainstalowane to samo oprogramowanie antywirusowe.
 - Oprogramowanie antywirusowe powinno mieć możliwość automatycznego (np. Zgodnie z harmonogramem) i ręcznego skanowania z generowaniem raportów wyników skanowania. Automatyczne skanowanie podłączonych urządzeń peryferyjnych (np. pamięci USB) jest wymagane przed ich użyciem.
 - Zainstalowane oprogramowanie powinno mieć możliwość zdalnej konfiguracji.
 - Dostarczenie, zainstalowanie i wdrożenie centralnej konsoli zarządzającej oprogramowaniem antywirusowym na wszystkich stacjach komputerowych lub serwerach ICS.
 - Centralne zarządzanie z jednego miejsca (tj. Automatyczne zmiany w konfiguracji / aktualizacji dla wszystkich innych stacji operacyjnych).
 - Wyłączanie, odinstalowanie lub zmiana konfiguracji systemu antywirusowego systemu ICS powinna być możliwa jedynie przez administratora systemu ICS.
- d. Compliance – Zgodność ze standardem PKN ORLEN w szczególności:
- Rozwiązanie, musi umożliwiać wizualizację bieżącego stanu zainstalowanych aktualizacji/poprawek aplikacji i systemu operacyjnego w odniesieniu do aktualnie zalecanych przez producenta systemu ICS na wszystkich składnikach ICS oraz bieżący stan bazy sygnatur antywirusowych w odniesieniu do aktualnie zalecanych przez producenta systemu ICS.
- e. Jump Server w szczególności:
- Jump Server musi być zainstalowany na infrastrukturze Zamawiającego;
- f. Autoryzacja i autentykacja:
- Zdalne zarządzanie stacjami komputerowymi ICS i serwerami (w tym kontami użytkowników, zasadami haseł, dostępem itp.) powinno być realizowane przez dedykowane kontrolery domeny umieszczony w strefie OT.
 - W systemie ICS muszą być zaimplementowane jedynie konta niezbędne do prawidłowego eksploatacji systemu ICS (konta nadmiarowe powinny być usunięte lub zablokowane).
 - Domyślne konta systemu operacyjnego muszą być usunięte lub zablokowane.
 - Administratorzy systemu ICS muszą mieć zdefiniowane wyłącznie konta imienne.
 - W komponenty systemu ICS pracujące pod kontrolą domeny nie powinno się stosować kont lokalnych.
 - Konta użytkowników powinny mieć zablokowaną funkcjonalność zdalnego logowania.
 - Domyślne hasła muszą być zmienione.

- Wdrożona polityka do zarządzania hasłami powinna być konstruowana z uwzględnieniem poniższych wymagań:
 - Długość, co najmniej 8 znaków dla standardowego konta Użytkownika.
 - Długość, co najmniej 12 znaków dla konta uprzywilejowanego.
 - Zastosowanie, co najmniej 3 z 4 grup znaków tj. mała litera (a-z), duża litera (A-Z), cyfra (0-9), znak specjalny (np. %, #, @, &, <, ^).
- g. System zbierania logów z komponentów ICS oraz przesyłania logów do centralnego rozwiązania klasy SIEM
 - Rozwiązanie musi zapewniać zbieranie logów ze stacji komputerowych, serwerów, urządzeń sieciowych, oprogramowania antywirusowego, macierzy dyskowych, środowiska wirtualnego systemów ICS.
 - Rozwiązanie musi umożliwiać przekazywanie logów z komponentów systemów ICS poprzez rozwiązanie (np. serwer logów) umieszczone w strefie DMZ OT do centralnej instancji systemu klasy SIEM. Dodatkowo rozwiązanie to musi zapewniać możliwość identyfikacji źródła z którego pochodzą logi.
 - Wraz z rozwiązaniem powinny być dostarczone propozycje i dobre praktyki związane z regułami korelacyjnych, alarmowaniem i wizualizacją, implementowaniem źródeł
 - Rozwiązanie musi współpracować/integrować z rozwiązaniami klasy SIEM wiodących i uznanych producentów.
- h. Infrastruktura:
 - Wykonawca musi dokonać oznaczenia okablowanie w systemie ICS z dwóch jego końców w sposób trwały zgodnie z wykorzystywanym nazewnictwem.
- i. Sieci w szczególności:
 - Zapewnienie pełnej ochrony pomiędzy strefą IT, strefą OT DMZ i strefą OT;
 - Projektowanie i wdrażanie separacji i segmentacji sieci ICS stosownie do standardów cyberbezpieczeństwa (takich jak NIST, ISA99).
 - Dostęp do sieci OT może być realizowany jedynie zgodnie z zasadami określonymi przez Dział Bezpieczeństwa IT.
 - Bezpośredni dostęp z sieci zewnętrznych do sieci OT (w której zaimplementowany jest system ICS) jest zabroniony.
 - Sieci teleinformatyczne systemu ICS muszą być odseparowane od innych sieci (w tym sieci korporacyjnych) za pomocą dedykowanych firewalli dostarczanych przez Zamawiającego.
 - Sieci teleinformatyczne poszczególny systemów ICS muszą być odseparowane od siebie a przepływ informacji pomiędzy nimi kontrolowany;
 - Nadmiarowy ruch generowany przez system ICS musi być usuwany u źródła tego ruchu (miedzy innymi: ruch do sieci Internet, niewykorzystywany ruch , nadmiarowy ruch pomiędzy podsieciami, nadmiarowy ruch wewnątrz podsieci).
 - Wszystkie przełączniki dostarczone do ICS muszą posiadać wszystkie porty o przepustowości min. 1 GB,
 - Wszystkie przełączniki dostarczane do ICS muszą być konfigurowalne, np; umożliwiając wyłączenia nieużywanych portów, zablokowania nieużywanych kont;
 - Funkcjonalność Switch Port Analyzer (SPAN) zwany także mirror port (umożliwiającym zrzucenie ruchu sieciowego ze wszystkich innych portów do jednego portu) musi zostać skonfigurowany na przełącznikach ICS. Porty SPAN / Mirror muszą

działać bez wpływu na wydajność i poprawność działania ICS oraz umożliwiać podłączenie niezależnych rozwiązań.

- Wszystkie przełączniki dostarczone do ICS muszą być skonfigurowane zgodnie z zasadami cyberbezpieczeństwa m.in. wyłączenia nieużywanych portów, zablokowania nieużywanych kont, konfiguracja przełączników tylko poprzez szyfrowane protokoły.
- j. Poświadczenia bezpieczeństwa w szczególności:
- Wszystkie nazwy użytkowników z hasłami dostępu zostaną przekazane do upoważnionych osób w PKN ORLEN wraz z przekazaniem kompletnego rozwiązania (w tym administratora, wymagane do prac serwisowych i wszystkich innych niezbędnych do działania ICS)
 - Wszystkie poświadczenia bezpieczeństwa (nazwy użytkowników wraz z hasłami) wykorzystywane w systemie ICS powinny być umieszczone w systemie zarządzania poświadczeniami bezpieczeństwa ORLEN bez zbędnej zwłoki.
 - wszystkie domyślne hasła należy zmienić przed uruchomieniem systemu.
- k. wymiana danych z systemami zewnętrznymi w szczególności:
- Wymiana danych z systemami zewnętrznymi powinna odbywać się przy użyciu standardu OPC i dedykowanego serwera zainstalowanego w strefie OT DMZ.
2. Zdalny dostęp do ICS
- a. każdy dostęp zdalny do ICS może być realizowany tylko dla zdefiniowanych / indywidualnych komputerów z wykorzystaniem dedykowanego rozwiązania zainstalowanego na infrastrukturze Zamawiającego (np. Jump server).
 - b. Zdalny dostęp musi zostać zatwierdzony przez Właściciela Biznesowego oraz Działu Bezpieczeństwa IT PKN ORLEN.
 - c. Zdalny dostęp musi być zgodny ze standardem i wymaganiami Działu Bezpieczeństwa IT PKN ORLEN. Podpisanie standardowego porozumienia PKN ORLEN o zdalnym dostępie jest niezbędne do uruchomienia zdalnego dostępu.
 - d. Zdalny dostęp do ICS jest możliwy tylko przy użyciu dedykowanego oprogramowania/stacji przesiadkowych.
 - e. Zdalny dostęp będzie realizowany wyłącznie za pomocą urządzeń działających w infrastrukturze PKN ORLEN i kontrolowanych wyłącznie za pośrednictwem odpowiedzialnych administratorów PKN ORLEN.
3. Dokumentacja techniczna cyberbezpieczeństwa
- a. Wykonawca musi przygotować i przekazać do Działu Bezpieczeństwa IT niezależną dokumentację techniczną (na etapie wdrożeniową oraz powykonawczą) obejmującą wszystkie aspekty cyberbezpieczeństwa i architektury ICS zgodnie z:
 - zasadami i przepisami obowiązującymi w Polsce,
 - wytycznymi PKN ORLEN w zakresie cyberbezpieczeństwa.
 - b. Niezależna dokumentacja obejmująca wszystkie aspekty cyberbezpieczeństwa i architektury ICS musi zostać uzgodniona oraz pozytywnie zaakceptowana przez Dział Bezpieczeństwa IT.
 - c. Niezależna dokumentacja techniczną cyberbezpieczeństwa musi zawierać między innymi:

- i. Architektura połączeń pomiędzy poszczególnymi komponentami systemu i systemami zewnętrznymi obejmująca między innymi adresację, wykorzystywane numery portów i protokoły
 - ii. Konfigurację urządzeń komputerowych, w tym między innymi:
 - Ustawienia systemu operacyjnego
 - Konta użytkowników i uprawnienia
 - Partycjonowanie dysku z konfiguracją
 - Ustawienia karty sieciowej
 - Konfiguracja firewall-i na poziomie systemu operacyjnego lub aplikacyjnym
 - Oprogramowanie (planowane / zainstalowane / uruchomione na poszczególnych zasobach)
 - Usługi (planowane / uruchomione w podziale na poszczególnych zasoby oraz aplikacje)
 - Porty (planowane do otwarcia/ otwarte w podziale na poszczególne zasoby oraz aplikacje)
 - Konfiguracja oprogramowania antywirusowego
 - Ustawienia portów USB i napędów CD / DVD w systemie OS (zwykle wyłączone z możliwością odblokowania przez administratora)
 - Ustawienia BIOS (w tym ustawienie hasła, opcja blokady USB)
 - lokalne zasady bezpieczeństwa LPO i zasady GPO
 - Procedury i polityka tworzenia kopii zapasowych
 - iii. Konfigurację sterowników, urządzeń PLC itp.
 - Konfiguracja kart komunikacyjnych
 - Protokoły i kanały komunikacji (np. ze stacjami komputerowymi)
 - Dostęp do urządzeń zarówno inżynierski jak i do danych
 - Zasady oprogramowania i aktualizacji
 - Konta użytkowników i uprawnienia
 - iv. System kopii zapasowych, w tym konfiguracja systemu backupowego, konfiguracja zasad tworzenia kopii zapasowych i ich alokacja do poszczególnych zasobów, spodziewane maksymalne obciążenie sieci, przewidywany czas utworzenia kopii zapasowej.
 - v. System antywirusowy, w tym, między innymi, jego konfiguracja w podziale na poszczególne zasoby.
 - vi. Proces aktualizacji systemów operacyjnych
 - vii. Procedury obejmujące między innymi
 - Procedury tworzenia kopii zapasowych.
 - Procedura aktualizacji bazy szczepionek antywirusa i oprogramowania antywirusowego.
 - Procedura aktualizacji systemu operacyjnego.
4. Kopie zapasowe
- a. Dostawca musi dostarczyć kopię bezpieczeństwa z bieżącą konfiguracją ICS.
 - b. Kopie zapasowe obejmują:
 - System operacyjny,
 - Oprogramowanie systemowe i narzędzia programowe,
 - Oprogramowanie,

- Sterowniki,
 - Inne oprogramowanie niezbędne do działania ICS,
 - Dane
- c. Wykonawca dostarczy instrukcje dotyczące tworzenia kopii zapasowych i odzyskiwania całego zainstalowanego oprogramowania ICS.
- d. ICS będzie wyposażony w narzędzia do wykonywania kopii zapasowych i odzyskiwania.
- e. Rozwiązanie do automatycznego wykonywania backupu stacji roboczych i serwerów ICS musi zostać zaprojektowane i zaimplementowane. System kopii zapasowych musi umożliwiać: automatyczne wykonywanie backupu zgodnie z wprowadzonym planem, ręczne przywracanie i tworzenie kopii zapasowych, weryfikację poprawności wykonania kopii zapasowych i przekazywanie informacji administratorowi, dokonywanie zmian konfiguracyjnych.