Grupa BZK

Wymagania IT dla dostawców systemów przemysłowych oraz automatyki

V3.4

2020-12-09

Spis treści

I. Cel

W celu zapewnienia integralności systemów teleinformatycznych oraz jednolitych standardów cyberbezpieczeństwa w systemach i sieciach automatyki przemysłowej wprowadza się poniższe zasady obowiązujące dla wszystkich wykonawców instalacji, firm serwisujące, oraz dostawców rozwiązań i urządzeń automatyki przemysłowej.

II. Ogólne zasady bezpieczeństwa

1. Brak możliwości podłączania jakichkolwiek urządzeń bezpośrednio do sieci Internet.
2. Brak możliwości łączenia bezpośredniego urządzeń do sieci przemysłowej OT i teleinformatycznej IT.
3. Włączanie urządzeń do infrastruktury teleinformatycznej Grupy BZK tylko w uzgodnieniu z Biurem Cyberbezpieczeństwa OT.
4. Nadawanie adresacji i innych parametrów konfiguracyjnych urządzeń sieciowych, które będą miały połączenie z infrastrukturą teleinformatyczną spółki, w tym sterowników, komputerów, itd. w uzgodnieniu z Biurem Cyberbezpieczeństwa OT.
5. Na serwerach i stacjach końcowych musi być zainstalowane oprogramowanie antywirusowe zgodne z obowiązującym standardem w Grupie BZK. W przypadku kiedy nie ma ono wsparcia dostawcy systemu automatyki, dla którego ma być zastosowane, należy zastosować kompatybilne z instalowanym systemem.
6. Stosowanie zasady minimalnych uprawnień. Rozdzielenie grup użytkowników w zależności od sprawowanej funkcji. Uruchamianie aplikacji bez uprawnień administratora.
7. Nie wykorzystywanie w systemach automatyki przemysłowej domyślnych , ani nieskomplikowanych haseł. Wymagania min. 12 znaków, wykorzystujące przynajmniej trzy spośród wymienionych elementów: duże litery, małe litery, cyfry, znaki specjalne.
8. Dla systemów krytycznych z punktu widzenia funkcjonowania przemysłowych systemów sterowania i automatyki należy zapewnić:
    a. aktywne wsparcie producenta zarówno dla sprzętu, jak i systemów operacyjnych i oprogramowania,
    b. automatyczne backupy danych o określonym harmonogramie i retencji,
    c. redundancję kluczowych elementów w celu wyeliminowania pojedynczych punktów awarii,
    d. plany odtworzenia funkcjonalności poszczególnych elementów i całych systemów w kontekście działalności przedsiębiorstwa – plany BCP/DRP – Business Continuity Plan/ Disaster Recovery Plan
    e. zapewnić archiwizację w bezpiecznym miejscu kluczowych informacji, w tym kodów programów PLC, konfiguracji, oprogramowania, narzędzi i systemów operacyjnych w celu odtworzenie systemu przemysłowego po awarii.
9. Wykonawca ma prawo zgłosić propozycję odstępstwa od zasad zapisanych w niniejszym dokumencie, jeżeli zachodzą ku temu uzasadnione przesłanki. Propozycja zmiany wraz uzasadnieniem musi zostać wysłana Użytkownika (Zamawiającego) i Biura Cyberbezpieczeństwa OT i uzyskać ich formalną akceptację. *Przykładową uzasadnioną przesłanką jest odstępstwo z uwagi na niestabilne działanie systemu / instalacji.*

III. Zdalny dostęp serwisowy

1. Dostęp zdalny do instalacji tylko za pośrednictwem dostarczonego przez Dział IT rozwiązania SSLVPN (Secure Socket Layer - Virtual Private Network) umożliwiającego zdalny dostęp do komputera za pomocą protokołu RDP (Remote Desktop Protocol).
2. Prace serwisowe są rejestrowane przez narzędzie do nagrywania sesji.
3. Uzyskanie zdalnego dostępu serwisowego do infrastruktury OT Grupy BZK wymaga obustronnego podpisania „Umowy udzielenia zdalnego dostępu serwisowego".
4. Wykonawca instalacji jest zobowiązany do dostarczenia stacji inżynierskiej w ramach realizowanej inwestycji w celu świadczenia zdalnego serwisu, jeżeli Zamawiający (Użytkownik) taką nie dysponuje. Parametry komputera przeznaczonego na stację inżynierską muszą być zaakceptowane przez Biuro Cyberbezpieczeństwa OT.

IV. Struktura połączeń i architektura systemu

1. Architektura systemu automatyki musi być przedstawiona do akceptacji Zamawiającego (Użytkownika) i Biura Cyberbezpieczeństwa OT przed rozpoczęciem wdrożenia. Propozycje zmian, które wynikną w trakcie realizacji prac muszą być przesłane wraz z uzasadnieniem do ponownej akceptacji przez Zamawiającego i Biuro Cyberbezpieczeństwa OT.
2. Przy projektowaniu sieci przemysłowej oraz dostawie urządzeń automatyki należy kierować się zasadami:
    a. sieć systemów przemysłowych jest wydzielona,
    b. przepływ danych pomiędzy siecią przemysłową, a infrastrukturą teleinformatyczną jest kontrolowany przez urządzenia typu firewall,
    c. systemy / zasoby, które powinny być dostępne w sieci teleinformatycznej i sieci przemysłowej mają być umieszone w strefie DMZ,
3. Adresacja IP wszystkich urządzeń wyposażonych w interfejs Ethernet musi być ustalona z Biurem Cyberbezpieczeństwa OT i zgodna ze stosowaną u Zamawiającego (Użytkownika).
4. Projektując połączenia należy stosować standaryzację protokołów komunikacyjnych, zgodnie z już wykorzystywanymi w danej fabryce protokołami.
5. Połączenia Ethernet urządzeń powinny być zaprojektowane i zrealizowane z wykorzystaniem kabli sieciowych min. kategorii 6 FTP lub kabli wyższej kategorii rekomendowanych przez producenta urządzeń.

V. Sterowniki PLC, panele operatorskie, bramy komunikacyjne i inne urządzenia z Interface Ethernet

1. Sterowniki PLC, panele operatorskie i inne urządzenia z interfejsem Ethernet muszą być zaakceptowane przez Zamawiającego (Użytkownika) i Biuro Cyberbezpieczeństwa OT.
2. Programy sterowników, paneli operatorskich, projekty SCADA i pliki konfiguracyjne mają być przekazane w formie edytowalnej wraz z komentarzami w języku polskim.
3. Stosowane sterowniki PLC muszą posiadać dziesięcioletni okres wparcia technicznego i dostępności części zamiennych.

4. Komunikacja stacji operatorskiej/serwera SCADA i panelu HMI ze sterownikiem PLC powinna odbywać się w oparciu o protokół komunikacyjny zgodny ze standardem danej fabryki.
5. Sterowniki i urządzenia automatyki mają być programowane z jednej (tej samej) stacji inżynierskiej z oprogramowaniem narzędziowym dla zachowania tej samej wersji oprogramowania.
6. Sterowniki PLC, panele operatorskie, moduły komunikacyjne itp. powinny mieć zainstalowaną najnowszą udostępnioną przez producenta wersję firmware na czas oddania instalacji.
7. Wyłączenie w sterownikach niewykorzystywanych funkcjonalności np. Serwer FTP, Web Serwer itp.
8. Ostatnią wersję programu sterownika należy wgrać do pamięci typu FLASH, niewymagającej podtrzymania bateryjnego.

VI. System operacyjny

1. Oprogramowanie przemysłowe ma być instalowane na najnowszych wspieranych przez producenta systemach operacyjnych na czas oddania instalacji.
2. Oprogramowanie przemysłowe nie może być instalowane na preinstalowanych systemach producenta sprzętu komputerowego (Dell, Lenovo, HP itp.). Na stacjach i serwerach ma być instalowane niezbędne do działania oprogramowanie, bez aplikacji typu gry, komunikatory itp.
3. System operacyjny powinien mieć zainstalowane wszystkie dostępne na stronie producenta aktualizacje systemowe, sterowniki, programy i pakiety zabezpieczeń zwalidowane przez producenta systemu automatyki, który będzie na nim zainstalowany.
4. W przypadku serwerowych systemów operacyjnych należy instalować angielską wersję językową.
5. Stacje operatorskie/serwery powinny być włączone do kontrolera domeny. Wykonawca instalacji ma poinformować o wymaganych politykach dla kontrolera domeny, w celu stabilnego działania aplikacji przemysłowej.
6. Stacje operatorskie/serwery powinny mieć zapewnioną ochronę antywirusową zgodną z zaleceniami Biura Cyberbezpieczeństwa OT
7. Aplikacja SCADA musi być uruchamiana na użytkownikach domenowych z ograniczonymi uprawnieniami. Nie dopuszczalna jest praca aplikacji wyłącznie na koncie z uprawnieniami administratora.
8. Jeżeli zachodzą uzasadnione przesłanki do odstępstwa od ww. zasad wymagana jest formalna akceptacja Użytkownika Końcowego oprogramowania i Biura Cyberbezpieczeństwa OT.

VII. Systemy SCADA/DCS

1. Dostarczane systemy przemysłowe, w szczególności oprogramowania przemysłowego, powinny być w najnowszych oferowanych przez producenta wersjach na czas oddania instalacji.

2. Rozdzielenie grup użytkowników w zależności od sprawowanej funkcji. Stosowanie zasady minimalnych uprawnień.
3. Aplikacja powinna być zintegrowana z Domeną BZK. Użytkownicy powinni logować się do aplikacji kontami domenowymi.
4. Włączenie do domeny, przydzielenie grup użytkowników należy ustalić z Biurem Cyberbezpieczeństwa OT.
5. Jeżeli zachodzą uzasadnione przesłanki do odstępstwa od ww. zasad wymagana jest formalna akceptacja Użytkownika Końcowego oprogramowania i Biura Cyberbezpieczeństwa OT.

VIII. Urządzenia sieciowe

1. Urządzenia sieciowe muszą być zaakceptowane przez Zamawiającego (Użytkownika) i Biuro Cyberbezpieczeństwa OT przed rozpoczęciem prac.
2. W celu zapewnienia możliwości monitorowania sieci OT pod względem anomalii i zagrożeń, należy dostarczyć zarządzalne przełączniki Ethernet i skonfigurować na każdym z nich mechanizm „port mirror" (SPAN) uwzględniający wszystkie przesyłane pakiety zarówno wysyłane jak i odbierane. Ustalenia w zakresie konfiguracji mają być zaakceptowane przez Biuro Cyberbezpieczeństwa OT.
3. Należy zapewnić połączenie i/lub dedykowany VLAN do zarządzania urządzeniami. Urządzenia mają być dostarczone z dedykowanym oprogramowaniem do zarządzania i konfiguracji, chyba Zamawiający (Użytkownik) już je posiada.
4. Urządzenia sieciowe powinny mieć zainstalowaną najnowszą udostępnioną przez producenta wersję firmware na moment oddania instalacji.
5. Urządzenia włączane w istniejącą infrastrukturę pierścienia powinny być kompatybilne z pracującymi i mieć wgrany taki sam firmware.
6. Nieużywane porty w urządzeniach sieciowych powinny być zablokowane.
7. Urządzenia dostarczane w ramach nowych prac i modernizacji, mają być zgodne ze standardem obowiązującym u Zamawiającego (Użytkownika).
8. Urządzenia powinny być dobrane tak, aby zapewnić min. 15% wolnych portów komunikacyjnych po zakończeniu wdrożenia na potrzeby rozbudowy instalacji.
9. Wykonawca prowadzący prace polegające na instalacji okablowania przedstawi raport pomiarów dynamicznych torów transmisyjnych potwierdzający poprawność fizycznej instalacji dla przewodów miedzianych i światłowodowych.

IX. Dokumentacja powykonawcza

1. Wykonawca przekaże:
    a. instrukcję operatorską,
    b. logiczne i fizyczne schematy połączeń urządzeń,
    c. wykaz zamontowanych urządzeń, z podaniem nazwy instalacji, nazwy producenta urządzenia, modelu urządzenia, wersji firmware, adresu IP, nazwy i wersji oprogramowania narzędziowego,
    d. wykaz kont i haseł z podziałem na urządzenia,

   e. wykaz zainstalowanych licencji wraz dokumentem potwierdzającym prawo do korzystania z oprogramowania.
2. Wykonawca przekaże kopie zapasowe w wersjach edytowalnych, z komentarzami dla:
   a. programów PLC (pełna wersja z komentarzami i nazwami zmiennych),
   b. paneli operatorskich (wraz z nazwami zmiennych),
   c. aplikacji SCADA wraz z instrukcją odtworzenia systemu (instrukcja z informacją o dodatkowych programach do zainstalowania),
   d. kopie zapasowe konfiguracji urządzeń sieciowych,
   e. inne konfigurowalne urządzenia (falowniki, bramy komunikacyjne itp.).
3. Raport z pomiarów dynamicznych torów transmisyjnych potwierdzający poprawność fizycznej instalacji okablowania oraz zgodność parametrów z normami danej kategorii / klasy okablowania dla przewodów miedzianych i światłowodowych.