

Zalecenia dotyczące cyberbezpieczeństwa dla wdrażanych systemów informacyjnych oraz minimalnych wymagań instrukcji eksploatacji systemów wykorzystywanych do świadczenia usługi kluczowej

1. Zaleca się aby oprogramowanie systemu oraz zamontowane i uruchomione serwery, stacje operatorskie i inne urządzenia składające się na system podłączony do sieci OT (sieć przemysłowa) spełniały następujące wymagania w zakresie Cyberbezpieczeństwa, które zostaną zrealizowane przez Wykonawcę:
 - a) Wykonawca po wykonaniu systemu powinien dokonać skanowania podatności pod względem znanych podatności. Proces testów musi obejmować monitoring stabilności skanowanych systemów i być wykonany zgodnie z przedstawioną metodologią i zaakceptowaną przez Zamawiającego. Zamawiający zaleca wykonanie testów zgodnie z metodyką np. OWASP. Wykonany test podatności zostanie przedstawiony Zamawiającemu do zaakceptowania. W przypadku wykrytych podatności Wykonawca proponuje zespołowi CERT LWB rozwiązania techniczne umożliwiające podniesienie poziomu bezpieczeństwa. Po zaakceptowaniu rozwiązań Wykonawca jest odpowiedzialny za ich wdrożenie.
 - b) Wykonawca wykona kopię bezpieczeństwa wszystkich elementów składowych systemu oraz dokona jej sprawdzenia poprzez przywrócenie jej na urządzeniu. Z wykonanych prób sprawdzenia kopii zapasowych zostanie wystawiony protokół.
 - c) Komputery systemu sterowania i nadzoru winny mieć zainstalowane dedykowane oprogramowanie antywirusowe aktualizowane regularnie w zakresie aplikacji antywirusowej i sygnatur złośliwego oprogramowania. Aktualizacje powyżej wymienione powinny być możliwe przy wykorzystaniu bezpiecznego połączenia np. przez wykonanie pośredniczącego serwera aktualizacji zabezpieczonego zaporą sieciową oraz bez konieczności łączenia komputerów z siecią „Internet”. Wykonanie serwera aktualizacji leży w gestii Wykonawcy. Zamawiający udostępni możliwość skonfigurowania dostępu do serwera aktualizacji dla programu antywirusowego obecnie wdrożonego w firmie.
 - d) Zainstalowane wersje oprogramowania antywirusowego wraz z sygnaturami złośliwego oprogramowania winny mieć możliwość bieżącego walidowania. Za walidowanie oprogramowania w ramach wsparcia technicznego na czas trwania gwarancji odpowiedzialny jest Wykonawca.
 - e) Zainstalowane oprogramowanie w zakresie systemu operacyjnego winno posiadać możliwość instalowania aktualizacji i poprawek. Za dokonywanie aktualizacji systemu w ramach wsparcia technicznego na czas trwania gwarancji odpowiedzialny jest Wykonawca.
 - f) Wykonawca odpowiedzialny jest za monitorowanie zmian w zakresie zastosowanych aplikacji systemu sterowania i nadzoru w tym również oprogramowania komponentów składających się na system oraz poinformowania Zamawiającego o nowych aktualizacjach, poprawkach związane z cyberbezpieczeństwem systemu i wykrytych zagrożeniach lub lukach w systemie.

- g) Komputery systemu sterowania i nadzoru winny mieć możliwość zablokowania funkcjonowania portów USB, w zakresie innym niż potrzebny do prawidłowego funkcjonowania zainstalowanego oprogramowania np. odczytywanie elektronicznego „klucza” licencji. Komputery powinny umożliwiać stworzenie kont użytkowników, dla których w/w blokada portów USB będzie personalizowana np. pełny dostęp do USB dla konta Administratora, a ograniczony dla pozostałych.
- h) Zainstalowane oprogramowanie (system operacyjny, system sterowania i nadzoru) winno umożliwiać tworzenie spersonalizowanych kont użytkowników charakteryzujących się różnymi uprawnieniami w zakresie obsługi. Zamawiający wymaga co najmniej następujących grup użytkowników:
- Administrator – dostęp pełny w zakresie odczytu/zapisu/modyfikacji/usuwania danych systemu;
 - Użytkownik - dostęp ograniczony w zakresie odczytu/ zapisu danych systemu,
 - Operator – dostęp w zakresie odczytu danych systemu,
- i) Zainstalowane oprogramowanie (system operacyjny, system sterowania i nadzoru) winno umożliwiać tworzenie spersonalizowanych sesji zalogowanych użytkowników. Modyfikacja czasu sesji, po którym użytkownik będzie automatycznie wylogowywany powinna być możliwa przez Administratora systemu.
- j) Dostęp do zasobów serwera, aplikacji systemu sterowania i nadzoru winien być realizowany za pomocą bezpiecznego uwierzytelnienia użytkownika i szyfrowania transmisji.
- k) Zaleca się aby zainstalowane oprogramowanie (system operacyjny, system sterowania i nadzoru) automatycznie wymuszało cykliczną zmianę hasła dostępu dla poszczególnych użytkowników. Określenie parametrów haseł w zakresie ilości, wielkości i rodzaju znaków, czasu obowiązywania, a także ich zmiana lub ich unieważnienie należy umieścić w kompetencjach Administratora systemu.
- l) Zegary urządzeń systemu sterowania i nadzoru (komputery, sterowniki procesowe i inne) powinny być synchronizowane czasem z serwerów czasu eksploatowanych przez Zamawiającego. Zamawiający na etapie projektowania udostępni adres sieciowy serwera czasu. Komputery winny być wyposażone w narzędzie kontrolujące proces synchronizacji i umożliwiające generowanie raportów.
- m) Stworzenie tzw. Whitelisting dla oprogramowania zainstalowanego na komputerach systemu sterowania i nadzoru i przekazanie Zamawiającemu.
- n) W przypadku konieczności stosowania zewnętrznych nośników danych dokonanie ich spersonalizowania z automatyczną kontrolą nośników dopuszczonych do współpracy z komputerami systemu sterowania.
- o) Ograniczenie komunikacji spoza segmentu sieci, w której działają urządzenia systemu sterowania i nadzoru kompleksu do komunikacji realizowanej wyłącznie za pośrednictwem bezpiecznego środowiska pośredniczącego (np. DMZ, stacje przesiadkowe) funkcjonującego w sieci informatycznej Zamawiającego.
2. Wykona dokumentację systemów informatycznych w szczególności, plan utrzymania ciągłości działania systemów informatycznych oraz instrukcję eksploatacji systemów sterowania i nadzoru ściany kombajnowej dla każdego z zastosowanego oprogramowania oddzielnie. Założenia do wykonania instrukcji uzgodni z

Zamawiającym.

2. Minimalne wymagania zawartości merytorycznej instrukcji eksploatacji systemów

2.2. Opis architektury technicznej

Wyszczególnienie oraz opis powiązań wszystkich komponentów sprzętowych, systemowych i aplikacyjnych występujących lub wymaganych do poprawnej pracy aplikacji zgodnie z wymaganiami wydajności, funkcjonalności i bezpieczeństwa.

Komponenty innych dostawców - dla komponentów innych dostawców, należy dokładnie określić wykorzystywane i dopuszczalne wersje.

- Rysunek architektury systemu

Rysunek przedstawiający architekturę systemu z podziałem na poziomy

- Konfiguracja techniczna

Opis konfiguracji technicznej, obejmującej wszystkie urządzenia wdrożone lub zainstalowane w ramach budowy systemu.

2.3. Zasoby (assets) systemu.

Serwery, stacje operatorskie, stacje inż., kontrolery domeny, historian, system antywirusowy, system patchowania WSUS, Alarm management i ich parametry sprzętowe (producent, model, service tag, nazwy NETBIOS, procesor, pamięć, dyski, karty sieciowe, zasilanie, itp.), BIOS, system operacyjny (parametry jądra, wymagane usługi).

Dokumentacja szaf serwerowych (lista i rozłożenie elementów, połączenia wewnątrz szaf, połączenia komunikacyjne do/z szaf, schematy zasilania, bilans mocy, schemat magistrali systemowej)

Dokumentacja techniczna producenta – specyfikacje techniczne, manuale, instrukcje

2.4. Sieć

Każdy switch/router/firewall powinien mieć swoją dokumentację (model urządzenia, wersja software, adres IP, opis portów, oznaczenie portów wyłączonych, listing z konfiguracji urządzenia), listy ACL dla routera, tabela traffic flow.

Infrastruktura sieciowa - parametry sprzętowe (porty fibre channel, aktywne licencje, itp.), fabric, zoning, aliasy, itp.

2.5. Oprogramowanie

Opis konfiguracji technicznej, obejmującej wszystkie urządzenia wdrożone lub zainstalowane w ramach budowy systemu.

Lista komponentów funkcjonalnych (oprogramowania) – komponenty Systemu i ich ustawienia zaimplementowane w Zasobach (assetach) systemu DCS

2.6. Opis architektury logicznej

Schemat i opis powiązań logicznych poszczególnych komponentów i ich rolę w architekturze – jako minimum lista komponentów i ich funkcje.

2.7. Opis konfiguracji komponentów systemu

Opis musi obejmować ogół oprogramowania wdrożonego, zainstalowanego w ramach systemu za Zasobach.

Przykładowy zestaw wymaganych danych konfiguracyjnych dla Zasobu obejmuje: ustawienia Firewall OS, lista i wersja zainstalowanych aplikacji, dokumentacja serwisów systemowych, narzędzia, dokumentacja użytkowników i grup systemowych, dokumentacja polityk grupowych GPO, katalog instalacyjny, położenie plików konfiguracyjnych, pierwotne parametry konfiguracyjne i zmodyfikowane w procesie instalacji, położenie plików logów, położenie i opis innych kluczowych plików i katalogów, parametry instancji, itp.

„Hardening assetów” –ustawień firewall OS, dezaktywacja portów USB, napędów optycznych, jeśli jest AWL (Application White Listing),

W przypadku uzasadnionym zespół CERT LWB może podjąć decyzję o odstąpieniu z ww. zaleceń.