

Regulamin Zarządzania Bezpieczeństwem OT w Aquanet SA

Załącznik 3.

Regulamin zarządzania wdrażanymi i modernizowanymi systemami

1. Nowo wdrażane i modernizowane systemy muszą spełniać szereg wymagań związanych z bezpieczeństwem wybranych obszarów.
2. Obszar 1 - aktualność
 - a. Wszystkie systemy operacyjne i firmware urządzeń muszą posiadać w dniu odbioru wspierany przez producenta system operacyjny/firmware.
 - b. Stacje inżynierskie dostarczone wraz z systemem będą zawierały wszelkie oprogramowanie, które jest niezbędne do wykonywania typowych czynności serwisowych przez zamawiającego.
3. Obszar 2 – Konfiguracja
 - a. System musi umożliwiać wgranie zewnętrznych certyfikatów dla szyfrowanej komunikacji SSL/HTTPS. Certyfikaty zostaną dostarczone przez zamawiającego.
 - b. W przypadku wykorzystania TLS do komunikacji należy wyłączyć możliwość korzystania z TLS 1.0 i TLS 1.1.
 - c. Wszystkie urządzenia posiadające taką możliwość muszą mieć włączone SNMP V3 jeśli jest wymagane używanie tego protokołu w przeciwnym wypadku obsługa protokołu powinna zostać wyłączona.
 - d. Stacje operatorskie/inżynierskie oparte o system operacyjny Windows muszą mieć włączony protokół WMI.
 - e. Zarządzanie uprawnieniami musi opierać się o indywidualne konta użytkownika lub o opisane szczegółowo w systemie role. Stosowna dokumentacja opisu ról musi być dostarczona przez wykonawcę.
4. Obszar 3 – Architektura i Zabezpieczenia
 - a. Elementy infrastruktury sieciowej rozwiązania podłączone będą do VLAN wskazanych przez zamawiającego. Odrębnie elementy wykonawcze, serwery oraz stacje robocze.
 - b. Interfejsy MGM dla serwerów (iDRAC, Zarządzanie VM) podłączone zostaną do odrębnego VLAN wskazanego przez zamawiającego.
 - c. Wykonawca uzgodni z zamawiającym jaki system antywirusowy z jaką konfiguracją jest dozwolony do stosowania na stacjach roboczych użytkowników.
 - d. W przypadku wykorzystania komunikacji mobilnej (LTE) wymagane jest skorzystanie z APN dostarczonego przez Zamawiającego.
 - e. Systemy operacyjne i aplikacje muszą umożliwiać uwierzytelnienie użytkowników za pośrednictwem Microsoft Active Directory. Wykonawca uzgodni z zamawiającym zakres integracji przed wdrożeniem.
 - f. Wykonawca przygotuje politykę i konfigurację kopii zapasowych systemu na wskazanej przez zamawiającego platformie.
 - g. Przed odbiorem prac realizowanych przez wykonawcę mogą zostać przez zamawiającego wykonane skany podatności narzędziem Nessus. Zakres, termin i sposób wykonania zostanie uzgodniony z wykonawcą. Z wykonawcą zostaną omówione również wyniki skanowania oraz niezbędne działania mitygujące.

5. Obszar 4 – Komunikacja z sieciami innymi niż OT
 - a. W przypadku konieczności publikacji/wysyłania danych z systemu do sieci LAN biurowej Zamawiającego, możliwe będzie publikowanie danych wyłącznie za pomocą serwera pośredniczącego (raportowego) umieszczonego w DMZ_OT. Zabrania się tworzenia bezpośrednich połączeń do sieci IT.
 - b. W przypadku wysyłania danych do sieci zewnętrznych w stosunku do sieci OT dopuszczone jest to jedynie poprzez interfejsy firewall udostępnionego przez zamawiającego z wykorzystaniem filtrów aplikacyjnych zastosowanych protokołów.
 - c. Reguły firewall tworzone w ramach komunikacji z systemami spoza sieci OT muszą zawierać minimalną liczbę adresów IP (zalecane pojedyncze adresy IP), reguły filtrujące poszczególne aplikacje/protokoły.
6. Obszar 5 – dokumentowanie wdrożenia
 - a. Zamawiający wymaga udokumentowania w dokumentacji powykonawczej:
 - b. Adresacji IP i adresów MAC systemu i wszystkich jego komponentów (zarówno dla elementów podłączonych i nie podłączonych do infrastruktury).
 - c. Wskazania wszystkich usług które są uruchomione w systemie i urządzeniach wykonawczych
 - d. Wskazania za pomocą jakich protokołów wymagana jest komunikacja z systemem i pomiędzy jego elementami.
 - e. Wskazania konfiguracji firewall umożliwiającej pracę systemu i komunikację z poszczególnymi jego elementami.
 - f. Wskazanie nazw i wersji systemów operacyjnych i elementów kluczowego oprogramowania
 - g. Wskazanie lokalizacji fizycznej systemu
 - h. Opis stosowanej kryptografii w systemie, w tym komunikacji kanałów szyfrowanych
 - i. Zamawiający wymaga zmiany wszystkich standardowych haseł oraz przekazania w formie szyfrowanej bazy Keepass zabezpieczonej hasłem (pobieranie Keepas w najnowszej wersji wyłącznie ze strony autorów oprogramowania <https://keepass.info/>), wszystkich haseł systemu i jego elementów dostarczonych przez wykonawcę. Klucz do ochrony bazy Keepas musi zawierać minimum 12 znaków, w tym duże, małe litery, znaki specjalne i cyfry.
 - j. Wykonawca przygotuje i przedstawi:
 - i. Procedurę aktualizacji systemów operacyjnych
 - ii. Procedurę aktualizacji firmware urządzeń
 - iii. Procedurę zmiany konfiguracji systemów i urządzeń
 - iv. Procedurę wykonywania kopii bezpieczeństwa oraz przywracania systemów z kopii.
 - v. Scenariusze możliwych i prawdopodobnych awarii wraz z procedurami DRP dla uzgodnionych z zamawiającym scenariuszy awarii systemu. Minimum dla serwerów i stacji operatorskich opisujących wymianę sprzętu oraz instalację systemu z wykorzystaniem kopii zapasowych.
 - vi. Wykonawca przed odbiorem systemu przedstawi skany podatności dostarczonego rozwiązania. Zakres i konfiguracje skanów zostaną uzgodnione z zamawiającym. Wykonawca uzgodni z zamawiającym sposób remediacji zidentyfikowanych podatności przed odbiorem systemu.
7. Obszar 6 – Integracja z systemami bezpieczeństwa
 - a. Zamawiający wymaga aby systemu umożliwiały integrację z systemami bezpieczeństwa zamawiającego w zakresie:

- b. Możliwości przesłania logów z systemów i aplikacji (standard Syslog lub inny uzgodniony).
 - c. Możliwości przesłania kopii ruchu z dostarczanych urządzeń sieciowych za pomocą portu mirror ze wszystkich dostępnych portów na urządzeniu (SPAN port).
 - d. W przypadku dostępności API umożliwiającego dostęp do kluczowych danych systemu zamawiający wymaga uzgodnienia z osobami odpowiedzialnymi za bezpieczeństwo potrzebę, możliwości i wypracowanie zakresu potrzebnej integracji z systemami bezpieczeństwa.
 - e. Zamawiający wymaga uzgodnienia w zakresie możliwości innych integracji, w tym możliwości instalacji dodatkowych pakietów oprogramowania wskazanych przez zamawiającego.
 - f. Uzgodnienia dotyczące integracji z systemami bezpieczeństwa zostaną udokumentowane w postaci karty integracji wskazanej przez zamawiającego.
8. Obszar 7 – Uwierzytelnienie użytkowników
- a. Wszystkie systemy OT muszą zapewniać uwierzytelnienie użytkownika przed dostępem do danych w nich przetwarzanych.
 - b. Metody silnego uwierzytelnienia przyjęte do stosowania w Aquanet:
 - c. Jednorazowe kody SMS
 - d. Jednorazowe kody czasowe

Certyfikaty x.509

- e. Wiadomości push w aplikacjach uwierzytelniających
 - f. Minimalna złożoność haseł użytkowników dla systemów IT
 - g. Minimum 10 znaków
 - h. Zawiera przynajmniej znaki z trzech grup (duże litery, małe litery, znaki specjalne cyfry)
 - i. Okresowa zmiana nie rzadziej niż 60 dni (zalecane wymuszanie przez system)
 - j. Minimalna złożoność haseł administracyjnych dla systemów IT i OT
 - k. Minimum 16 znaków
 - l. Zawiera przynajmniej znaki z trzech grup (duże litery, małe litery, znaki specjalne cyfry). Zaleca się generowanie losowych ciągów znaków dla wszystkich haseł administracyjnych.
 - m. Okresowa zmiana nie rzadziej niż 60 dni (zalecane wymuszanie przez system)
 - n. Jeżeli jest to technicznie wykonalne, wszystkie konta administracyjne muszą stosować silne uwierzytelnienie
9. Obszar 8 – Stosowanie kryptografii
- a. Opracowane na podstawie Microsoft, NIST SP 800-57 oraz BSI TR-02102
 - b. Szyfrowanie komputerów/urządzeń mobilnych
 - c. Zaleca się wykorzystanie modułów TPM dla przechowywania kluczy w urządzeniach.
 - d. W przypadku korzystania z Bit Locker na stacjach Windows:
 - e. Wymagane jest szyfrowanie powierzchni całego dysku (full encryption method).
 - f. Wymagane jest użycie modułu TPM jeżeli komputer jest w niego wyposażony.
 - g. Zaleca się w celu szczególnej ochrony wybranych stacji stosowanie modułu TPM i ochrony kodem PIN/Kluczem. (TPM+PIN, TPM+startup key authentication method zgodnie z rekomendacjami Microsoft).
- Wersje TLS/SSL
- h. Należy stosować TLS przynajmniej w wersji 1.2

- i. Należy stosować biblioteki Open SSL przynajmniej w wersji 1.1.0
- j. Długość kluczy
 - Wymagane jest korzystanie z kluczy kryptograficznych o długości przynajmniej 2000 bit.
- k. Dopuszczone funkcje haszujące
 - SHA256, SHA384 lub SHA512
 - Diffie Hellman groups
- l. Dla tuneli VPN site to site wymagane jest stosowanie grup DH:
23,24,26,27,28,256,257,258
- m. Algorytmy symetryczne
 - Przy szyfrowaniu symetrycznym wymagane jest skorzystanie z protokołu AES 256