

Część 6 – Zakup oprogramowania do zarządzania bezpieczeństwem IT – DLP, monitoring zasobów zarządzania dostępem

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ) – SYSTEM ZARZĄDZANIA INFRASTRUKTURĄ IT I BEZPIECZEŃSTWEM DANYCH

Wymagania ogólne i architektura

1. System musi posiadać budowę modułową, umożliwiającą instalację i licencjonowanie wybranych funkcjonalności.
2. Architektura typu klient-serwer, składająca się z serwera zarządzającego, konsoli administratora (GUI) oraz agentów instalowanych na stacjach roboczych.
3. System musi posiadać wbudowaną bezpłatną bazę danych lub współpracować z bezpłatnymi silnikami bazodanowymi (np. PostgreSQL lub MS SQL Express). W przypadku rozwiązania opartego o MS SQL Express, Wykonawca gwarantuje, że przy monitorowaniu 80 stacji roboczych w pełnym zakresie (wraz z historią aktywności użytkowników przechowywaną przez min. 24 miesiące), nie dojdzie do przekroczenia limitów darmowej wersji bazy. W przeciwnym razie Wykonawca jest zobowiązany dostarczyć pełną licencję bazy danych w cenie oferty.
4. Komunikacja sieciowa pomiędzy wszystkimi komponentami systemu (Agentami, Serwerem Zarządzającym, Konsolami Administratora) musi być w pełni szyfrowana. Zamawiający wymaga zastosowania protokołu TLS w wersji co najmniej 1.2 (zalecana wersja 1.3). System nie może wymuszać stosowania przestarzałych i niebezpiecznych protokołów (SSL v3, TLS 1.0, TLS 1.1) do prawidłowego działania. W przypadku komunikacji Agent z Serwerem, szyfrowanie musi obejmować przesyłanie wszelkich danych inwentaryzacyjnych, informacji o aktywności użytkowników oraz poleceń administracyjnych.
5. Zamawiający wymaga dostarczenia licencji bezterminowej (wieczystej) na oprogramowanie. Licencja musi uprawniać do korzystania z oprogramowania w zakupionej wersji przez czas nieokreślony, nawet po wygaśnięciu wsparcia technicznego.
6. Licencjonowanie systemu musi być oparte na liczbie monitorowanych stacji roboczych (Agentów) z systemem operacyjnym Microsoft Windows.
 - a) Wymagana ilość licencji na stacje robocze (Agenty): co najmniej 80 sztuk.
 - b) Wymagana ilość licencji na urządzenia sieciowe monitorowane bezagentowo (np. drukarki, przełączniki, routery) poprzez protokół SNMP/ICMP: co najmniej 20 sztuk (lub nielimitowana).
 - c) Liczba administratorów/techników obsługujących system (Konsole Zarządzające): nielimitowana.
 - d) Licencja musi umożliwiać instalację Agentów na stacjach roboczych w dowolnej lokalizacji w ramach infrastruktury sieciowej Zamawiającego.

Załącznik nr 1.6

7. W cenie oferty Wykonawca musi zapewnić pakiet asysty technicznej i aktualizacji na okres 12 miesięcy od daty podpisu protokołu odbioru. Pakiet ten musi obejmować:
- a) Prawo do pobierania i instalacji wszystkich nowych wersji oprogramowania (upgrade) oraz poprawek bezpieczeństwa wydanych przez producenta w tym okresie.
 - b) Dostęp do pomocy technicznej świadczonej przez wykwalifikowanych inżynierów (Helpdesk) w języku polskim (poprzez telefon, e-mail lub dedykowany portal zgłoszeniowy).
 - c) Dostępność wsparcia: Świadczenie usług asysty technicznej oraz przyjmowanie zgłoszeń serwisowych musi być realizowane w dni robocze (od poniedziałku do piątku), z wyłączeniem dni ustawowo wolnych od pracy, w godzinach od 07:30 do 15:30.
 - d) W ramach asysty technicznej Wykonawca zobowiązany jest do udzielania wsparcia w zakresie diagnozy problemów z działaniem oprogramowania, konfiguracji modułów oraz wyjaśniania wątpliwości dotyczących funkcjonalności systemu.

Moduł Monitorowania Sieci

Cel: Zapewnienie ciągłości działania infrastruktury sieciowej i serwerowej.

- a) Wizualizacja sieci: System musi umożliwiać tworzenie graficznych map sieci z obsługą tła (np. rzutów pięter). Ikony urządzeń na mapie muszą zmieniać status w czasie rzeczywistym w zależności od dostępności urządzenia.
- b) Wykrywanie urządzeń: Automatyczne skanowanie sieci i wykrywanie podłączonych urządzeń (Discovery) w oparciu o zdefiniowane podsieci IP.
- c) Protokoły monitorowania: Obsługa protokołów ICMP (Ping), SNMP (v1, v2c, v3), WMI.
- d) Monitorowanie usług: Możliwość monitorowania dostępności usług sieciowych (np. HTTP, POP3, SMTP, FTP, SQL) wraz z czasem odpowiedzi.
- e) Monitorowanie przełączników (Switchy):
 - i. Odczyt informacji z przełączników zarządzalnych przez SNMP.
 - ii. Mapowanie portów (Port Mapper): informacja, do którego fizycznego portu switcha podłączone jest dane urządzenie końcowe (MAC/IP).
 - iii. Monitorowanie obciążenia portów (transfer, błędy pakietów).
- f) Powiadomienia: System alertów (e-mail, SMS lub komunikaty ekranowe) w przypadku awarii urządzenia, zatrzymania usługi lub przekroczenia zdefiniowanych progów wydajności (np. zużycie CPU, RAM, zajętość dysku na serwerach).
- g) Logi: Obsługa zbierania logów zdarzeń (Syslog) oraz Windows Event Log z wybranych maszyn.

Załącznik nr 1.6

Moduł Inwentaryzacji Zasobów

Cel: Automatyczna ewidencja sprzętu i oprogramowania oraz zarządzanie środkami trwałymi.

- a) Audyt sprzętu: Automatyczne zbieranie informacji o konfiguracji sprzętowej stacji roboczych (CPU, RAM, HDD, płyta główna, karty rozszerzeń, numery seryjne) za pomocą zainstalowanych agentów.
- b) Audyt oprogramowania: Automatyczne wykrywanie zainstalowanego oprogramowania, identyfikacja plików wykonywalnych i multimedialnych.
- c) Zarządzanie licencjami: Możliwość wprowadzania posiadanych licencji i automatyczne porównywanie ich z liczbą zainstalowanych aplikacji (kontrola legalności).
- d) Rejestr Środków Trwałych: Wbudowana baza danych do ewidencji sprzętu IT i non-IT (np. meble, telefony). Możliwość definiowania własnych atrybutów (np. data gwarancji, nr faktury, przypisany użytkownik).
- e) Historia zmian: Rejestrowanie historii zmian sprzętowych (np. wymiana kości pamięci, podmiana dysku) oraz instalacji/deinstalacji oprogramowania.
- f) Wsparcie dla kodów kreskowych/QR:
 - i. Możliwość generowania i druku etykiet inwentaryzacyjnych z kodami kreskowymi lub QR.
 - ii. Obsługa procesu inwentaryzacji (spis z natury) z wykorzystaniem urządzeń mobilnych (np. smartfon z systemem Android/iOS lub kolektor danych) integrujących się z bazą systemu.

Moduł Ochrony Danych

Cel: Ochrona przed wyciekiem danych (DLP) i zarządzanie nośnikami wymiennymi.

- 1. Kontrola nośników: Możliwość blokowania lub przydzielania praw dostępu (odczyt, zapis, wykonanie) do portów USB i nośników wymiennych (pendrive, dyski zewnętrzne).
- 2. Granulacja uprawnień: Prawa dostępu definiowane dla:
 - a) Całej organizacji (polityka globalna).
 - b) Grup użytkowników lub działów (np. integracja z Active Directory).
 - c) Konkretnych urządzeń (biała lista pendrive'ów autoryzowanych służbowo po numerze seryjnym/ID sprzętu).
- 3. Audyt operacji plikowych: Rejestrowanie operacji na plikach (kopiowanie, kasowanie, zmiana nazwy, otwarcie) dokonywanych na nośnikach przenośnych oraz (opcjonalnie) na udostępnionych zasobach sieciowych.

Załącznik nr 1.6

4. Integracja z systemem operacyjnym:

- a) Odczyt statusu szyfrowania dysków (np. BitLocker) i raportowanie stacji niezaszyfrowanych.
- b) Zarządzanie zaporą systemową z poziomu konsoli administratora.

5. Alarmy bezpieczeństwa: Powiadamianie administratora o podłączeniu nieautoryzowanego nośnika lub próbie skopiowania danych wbrew polityce.

Zakres wdrożenia

Zamawiający wymaga przeprowadzenia wdrożenia oprogramowania w formie zdalnej asysty technicznej w wymiarze do 8 roboczogodzin. Usługa obejmuje wsparcie administratorów Zamawiającego w instalacji serwera aplikacji, konfiguracji bazy danych oraz instruktaż w zakresie masowego wdrażania agentów (np. poprzez GPO Active Directory).

Wymagania w zakresie dostępności cyfrowej i projektowania uniwersalnego:

1. Dostarczone oprogramowanie w zakresie interfejsów użytkownika dostępnych przez przeglądarkę internetową (Web GUI) oraz generowanych raportów (np. PDF, HTML) musi być zgodne z wytycznymi WCAG 2.1 (Web Content Accessibility Guidelines) na poziomie AA, zgodnie z załącznikiem do ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych.
2. W szczególności interfejsy zarządzające powinny umożliwiać:
 - a) Obsługę podstawowych funkcji systemu za pomocą samej klawiatury (bez użycia myszy).
 - b) Skalowanie czcionek i zmianę kontrastu bez utraty funkcjonalności (dla osób słabowidzących).
 - c) Współpracę z powszechnie używanymi technologiami asystującymi (czytniki ekranu), o ile pozwala na to specyfika prezentowanych danych technicznych (np. wykresy, mapy topologii).
3. W przypadku aplikacji desktopowych (instalowanych na stacji roboczej), interfejs powinien wspierać systemowe ustawienia ułatwień dostępu (np. tryb wysokiego kontrastu systemu Windows, skalowanie DPI).