Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Spis treści

I. WPROWADZENIE

Przedmiotem zamówienia jest dostawa, wdrożenie (w tym instalacja) i uruchomienie modułowego systemu Data Loss Prevention, zwanego dalej: *„Oprogramowaniem”,* służącego do zapobiegania wyciekom danych w infrastrukturze IT Zamawiającego.

Zamówienie realizowane jest w ramach Inwestycji C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo - Cyberbezpieczny Rząd, finansowanej ze środków Krajowego Planu Odbudowy i Zwiększania Odporności finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności.

II. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Zakres Przedmiotu zamówienia

1.1 Wykonanie Przedmiotu zamówienia obejmuje:

a) dostawę, wdrożenie (w tym instalację) i uruchomienie modułowego Oprogramowania, służącego do zapobiegania wyciekom danych w infrastrukturze IT Zamawiającego;

b) realizację szkolenia z Oprogramowania.

1.2 Zamawiający wymaga dostarczenia 220 licencji (per użytkownik) na Oprogramowanie o minimalnym okresie obowiązywania wynoszącym 12 miesięcy.

2. Realizacja Przedmiotu zamówienia

2.1 W ramach realizacji Przedmiotu zamówienia Wykonawca zobowiązany jest do wykonania następujących prac:

a) instalacja Oprogramowania wraz z agentem i klientami na wybranych stacjach roboczych u Zamawiającego, w celu zbierania danych telemetrycznych;

b) przegląd i omówienie funkcjonalności;

c) analiza potencjalnych punktów wycieku danych oraz przeprowadzenie przykładowego audytu bezpieczeństwa;

d) opracowanie i wdrożenie minimum trzech klasyfikacji danych wrażliwych;

e) utworzenie i wdrożenie minimum trzech polityk DLP bazujących na wcześniej ustalonych klasyfikacjach;

f) optymalizacja konfiguracji Oprogramowania w celu zapewnienia wydajnego i stabilnego działania.

2.2 Oprogramowanie musi zapewniać centralne zarządzanie urządzeniami i użytkownikami Zamawiającego, egzekwowanie polityk bezpieczeństwa, analizę oraz blokowanie przesyłania danych chronionych, a także pełną integrację z istniejącą infrastrukturą IT Zamawiającego, zgodnie z wymaganiami funkcjonalnymi opisanymi w rozdziale III.

2.3 Oprogramowanie musi być zakupione w oficjalnym kanale dystrybucyjnym producenta i być objęte serwisem producenta lub autoryzowanego partnera serwisowego producenta na terenie Polski.

2.4 Dostarczona przez Wykonawcę licencja Oprogramowania, w okresie 12 miesięcy jej obowiązywania, powinna zapewniać usługi wsparcia producenta Oprogramowania, obejmujące m.in.: wsparcie techniczne producenta, maintenance, Software Assurance, możliwość uaktualnienia Oprogramowania do nowszych wersji oraz dostęp do aktualizacji.

2.5 Oferowane Oprogramowanie musi stanowić zintegrowaną, zamkniętą platformę, która do prawidłowego działania wszystkich funkcjonalności wymaga instalacji wyłącznie na jednej maszynie wirtualnej. Platforma musi zawierać całość niezbędnego oprogramowania (bazę danych, aplikacja). Wszystkie komponenty Oprogramowania, w tym licencje, nie mogą generować dodatkowych kosztów, a dostarczone licencje dla bazy danych muszą zapewniać zaawansowane funkcje centrum danych, nieograniczoną wirtualizację oraz wsparcie dla krytycznych obciążeń.

2.6 Wykonawca jest zobowiązany do dostarczenia kompletnego i działającego Oprogramowania, w tym wszystkich niezbędnych licencji (w tym system operacyjny), jeśli są one wymagane do jego prawidłowego funkcjonowania.

2.7 Wszelkie usługi wsparcia producenta Oprogramowania muszą rozpoczynać się w tym samym terminie, co uruchomienie licencji Oprogramowania. Termin ten nie może rozpocząć się wcześniej niż w dniu podpisania bez zastrzeżeń Protokołu Odbioru Oprogramowania. Wykonawca zobowiązany jest dołączyć do oferty oświadczenie, w którym potwierdzi, że aktywacja licencji Oprogramowania oraz wszystkich powiązanych z nią usług wsparcia producenta Oprogramowania nastąpi w tym samym terminie oraz że okres ich obowiązywania nie będzie krótszy niż 12 miesięcy.

2.8 Usługi wsparcia producenta Oprogramowania muszą być świadczone w języku polskim przez producenta Oprogramowania lub autoryzowanego partnera producenta — wymagane jest dostarczenie oświadczenia Wykonawcy potwierdzające, że wsparcie będzie realizowane przez Producenta lub autoryzowanego partnera producenta, które należy dołączyć do oferty.

III. SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Opis rozwiązań (wymagania minimalne)

1.1 Serwer zarządzający

1.1.1 Oprogramowanie musi zapewniać możliwość centralnego zarządzania stacjami roboczymi i serwerami.

1.1.2 Oprogramowanie musi wspierać przynajmniej następujące systemy operacyjne:

a. Windows 10/11 i nowszy.

b. MacOS 12.0 i nowszy.

1.1.3 Pomoc i dokumentacja muszą być dostępna przynajmniej w języku angielskim.

1.1.4 Konsola administracyjna musi pozwalać na pobranie instalatora w wersji offline – pozwalającego na wykonanie instalacji bez połączenia z Internetem.

1.1.5 Konsola administracyjna musi pozwalać na tworzenie dodatkowych kont Administracyjnych oraz innych użytkowników.

1.1.6 Konsola administracyjna musi pozwalać na przesyłanie powiadomień e-mail.

1.1.7 Konsola administracyjna musi pozwalać na weryfikację wersji zainstalowanego

oprogramowania klienta, a także umożliwia aktualizację do nowej wersji.

1.1.8 Konsola administracyjna musi udostępniać dziennik audytu wykonywanych operacji.

1.1.9 Konsola administracyjna musi umożliwiać przesyłanie danych do zewnętrznego serwera Syslog.

1.2 Reguły Oprogramowania Data Loss Prevention (DLP)

1.2.1 Oprogramowanie musi umożliwiać pracę w przynajmniej dwóch trybach: obserwacji, który nie ma wpływu na przesyłane dane oraz trybu egzekwowania, który przestrzega polityk DLP.

1.2.2 Reguły Oprogramowania muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.

1.2.3 Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.

1.2.4 Oprogramowanie musi pozwalać na blokadę stron internetowych po zdefiniowanej kategorii oraz umożliwiać tworzenie wyjątków w oparciu o adres URL.

1.2.5 Oprogramowanie musi przedstawiać podsumowanie przynajmniej dla zablokowanych zdarzeń po stronie użytkownika.

1.2.6 Oprogramowanie musi reagować na próby przesłania plików z chronioną zawartością przynajmniej w oparciu o:

a. Numer pesel,
b. Numer regon,
c. Numer paszportu,
d. Słowa kluczowe,
e. Zdefiniowane wyrażenia regularne.

1.2.7 Oprogramowanie musi umożliwiać tworzenie własnych detektorów zawartości.

1.2.8 Oprogramowanie musi posiadać przynajmniej 45 wbudowanych detektorów zawartości.

1.2.9 Oprogramowanie musi umożliwiać przesłanie chronionych danych po wprowadzeniu przez użytkownika uzasadnienia.

1.2.10 Oprogramowanie musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365.

1.2.11 Oprogramowanie musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla firm i Microsoft Teams.

1.2.12 Oprogramowanie musi wykonywać analizę OCR.

1.2.13 Oprogramowanie musi blokować przesyłanie plików z nieznaną zawartością, które zostały zaszyfrowane przy pomocy hasła.

1.2.14 Oprogramowanie musi umożliwiać utworzenie wyjątków dla istniejących reguł DLP.

1.2.15 Oprogramowanie musi blokować próbę przesłania danych w przypadku braku informacji, co do zawartości pliku.

1.2.16 Oprogramowanie musi umożliwiać przypisanie indywidualnej polityki dostępu, np.

umożliwiając przesyłanie danych do wskazanej lokalizacji.

1.2.17 Oprogramowanie musi umożliwiać blokowanie dostępu do urządzeń wymiennych i portów w tym przynajmniej portu USB.

1.2.18 Oprogramowanie musi umożliwiać tworzenie białych i czarnych list urządzeń dopuszczonych do użycia.

1.2.19 Oprogramowanie musi umożliwiać zablokowanie kopiowania danych do schowka w przypadku danych chronionych.

1.2.20 Oprogramowanie musi umożliwiać blokowanie wykonania zrzutu ekranu.

1.3 Powiadomienia i raportowanie

1.3.1 Oprogramowanie musi udostępniać generowanie raportu na podstawie wskazanego zakresu czasu.

1.3.2 Oprogramowanie musi udostępniać przynajmniej 5 wbudowanych raportów dotyczących DLP.

1.4 Wymagania dla wdrożenia Oprogramowania DLP

1.4.1 Instalacja i wstępna konfiguracja Oprogramowania

a. Zainstalowanie serwera DLP oraz agenta i klienta na stacjach końcowych, celem zbierania danych.

b. Omówienie kluczowych funkcji i obsługi konsoli administracyjnej Oprogramowania.

1.4.2 Analiza i klasyfikacja danych

a. Przeprowadzenie analizy potencjalnych miejsc wycieków danych.

b. Wygenerowanie przykładowego audytu.

c. Utworzenie klasyfikacji danych (do trzech kategorii).

1.4.3 Tworzenie i wdrażanie polityk DLP

a. Ustalenie oraz wdrożenie do trzech polityk egzekwowanych na stacjach końcowych, bazując na wcześniejszej klasyfikacji danych.

b. Optymalizacja działania Oprogramowania w oparciu o utworzone polityki.

1.4.4 Szczegółowy plan wdrożenia krok po kroku:

a. Instalacja i konfiguracja serwera wirtualnego DLP – uruchomienie oprogramowania zarządzającego w środowisku Zamawiającego.

b. Omówienie procedury instalacyjnej klientów DLP oraz przygotowanie zadania wdrożeniowego na wybranych stacjach roboczych.

c. Integracja z usługą Active Directory – synchronizacja z istniejącą strukturą użytkowników i zasobów.

d. Prezentacja funkcjonalności konsoli zarządzającej.

e. Analiza środowiska IT oraz aktywacja funkcji audytowania.

f. Przeprowadzenie podstawowej analizy potencjalnych wycieków danych na maksymalnie jednej stacji roboczej.

g. Wygenerowanie przykładowego raportu audytowego z uwzględnieniem wykrytych zdarzeń.
h. Konfiguracja klasyfikacji danych wrażliwych (maksymalnie trzech), bazując na informacjach wskazanych przez Zamawiającego.
i. Wdrożenie polityk DLP (maksymalnie trzech) dotyczących m.in. pochodzenia pliku, zawartości pliku lub jego właściwości.
j. Konfiguracja kontroli dostępu do stron WWW oraz urządzeń przenośnych.
k. Finalne testy systemu i optymalizacja ustawień – weryfikacja skuteczności oraz wydajności wdrożonego rozwiązania.

2. Szkolenia

1.4.5 Szkolenie musi być prowadzone przez trenera certyfikowanego w zakresie proponowanego Oprogramowania. Wykonawca, na etapie realizacji umowy, na żądanie Zamawiającego, przedstawi kopię certyfikatu trenera.

1.4.6 Trener zapewni szkolenie w oparciu o wdrożone Oprogramowanie u Zamawiającego.

1.4.7 Szkolenie musi być zorganizowane dla 3 osób.

1.4.8 Wykonawca zobowiązuje się do przeprowadzenia dwóch dni szkoleniowych, min. 14 godzin szkolenia (proponowany podział: 2 dni po 7 godzin).

1.4.9 Szkolenie musi obejmować teoretyczne i praktyczne aspekty pracy z Oprogramowaniem, w tym:

a. Wdrożenie i konfiguracja Oprogramowania,
b. Instalacja i wdrożenie serwera DLP,
c. Instalacja i wdrożenie klienta DLP na stacjach roboczych,
d. Zarządzanie i kategoryzacja:
   - Kategoryzacja aplikacji oraz stron internetowych,
   - Zarządzanie bazą danych użytkowników, urządzeń lub zagrożeń,
   - Ustawienia oraz personalizacja klienta DLP,
   - Dezaktywacja oraz zarządzanie modułami klienta DLP,
   - Konfiguracja i ustawienia integracji DLP z innymi systemami.
e. Analiza i wykrywanie incydentów:
   - Uruchomienie oraz obsługa modułu Discovery (automatyczne wykrywanie zasobów i danych),
   - Analiza potencjalnych wycieków danych (identyfikacja miejsc i przyczyn),
   - Dostosowanie konsoli DLP do własnych potrzeb: personalizacja pulpitu, filtrowanie danych i widoków.
f. Ochrona danych i dostępów:
   - Szyfrowanie dysków przy użyciu Bitlockera,
   - Strefy bezpieczeństwa – konfiguracja dostępów dla urządzeń i portów, m.in.

USB.

g. Reguły polityk DLP i monitorowanie:
   - Tryby polityk: omówienie i wdrożenie reguł DLP (w tym tryb monitorowania i tryb egzekwowania),
   - Tworzenie i zarządzanie regułami ogólnymi (np. na poziomie całej organizacji),
   - Tworzenie i zarządzanie regułami aplikacyjnymi (np. specyficznymi dla danej aplikacji czy grupy użytkowników),
   - Inteligentne wykrywanie danych osobowych (automatyczne rozpoznawanie i klasyfikowanie danych wrażliwych),
   - Dzienniki DLP (audit log) – przegląd, analiza oraz zarządzanie zapisami aktywności i incydentów.

3. DNSH (Do No Significant Harm)

Przedmiot zamówienia mus być zgodny z zasadą „niewyrządzania znaczącej szkody" (Do No Significant Harm – DNSH). Oznacza to, że Wykonawca musi zapewnić, że jego realizacja nie będzie miała znaczącego negatywnego wpływu na cele środowiskowe, takie jak ochrona klimatu, gospodarka o obiegu zamkniętym, zapobieganie zanieczyszczeniom oraz ochrona bioróżnorodności. Wszystkie wdrażane rozwiązania zostały zaprojektowane w sposób minimalizujący negatywny wpływ na środowisko naturalne.