Załącznik nr 1C do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Spis treści

I. WPROWADZENIE

Przedmiotem zamówienia jest dostawa i wdrożenie kompleksowego rozwiązania bezpieczeństwa dla styku sieci Internet z usługami wewnętrznymi Zamawiającego (dalej: „*Oprogramowanie*" lub *„WAF"*).

Zamówienie finansowane w ramach Krajowego Planu Odbudowy i Zwiększania Odporności finansowanego ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności (dalej: „KPO"), Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo Cyberbezpieczeństwo - Cyberbezpieczny Rząd.

II. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Zakres Przedmiotu zamówienia

1.1. Wykonanie Przedmiotu zamówienia obejmuje:

a) dostawę kompleksowego Oprogramowania w celu zapewnienia bezpieczeństwa dla styku sieci Internet z usługami wewnętrznymi Zamawiającego;

b) realizację wdrożenia (w tym instalacji) i uruchomienia Oprogramowania;

c) realizację szkolenia z Oprogramowania.

1.2. Oprogramowanie ma pełnić rolę zaawansowanej bramy aplikacyjnej (Application Delivery Controller), której kluczowymi zadaniami są ochrona publikowanych serwisów poprzez zintegrowaną Zaporę Aplikacji Webowych (WAF) oraz zapewnienie ich wysokiej dostępności i optymalnej wydajności dzięki funkcjonalności równoważenia obciążenia (Load Balancing). Dostarczone Oprogramowanie musi zapewniać funkcjonowanie jako klaster wysokiej dostępności (HA) w formie wirtualnych urządzeń.

1.3. Zamawiający wymaga dostarczenia licencji na Oprogramowanie o minimalnym okresie obowiązywania wynoszącym 12 miesięcy ze wsparciem na 12 miesięcy. Okres trwania licencji przez Wykonawcę (subskrypcja na 12 miesięcy lub wieczysta) podlega ocenie w ramach kryteriów oceny ofert.

2. Realizacja Przedmiotu zamówienia

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

2.2. Niezależnie od dostarczonej przez Wykonawcę licencji Oprogramowania (subskrypcji na 12 miesięcy lub wieczystej), każda z nich, 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.

2.3. 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.

2.4. 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. Zaawansowana Ochrona Aplikacji (Web Application Firewall - WAF):

1.1.1. Integralność i ochrona: Każda instancja wchodząca w skład klastra musi posiadać w pełni zintegrowany, wbudowany moduł zapory sieciowej dla aplikacji webowych (WAF). Moduł WAF musi chronić aplikacje i serwisy przed szerokim spektrum zagrożeń, w tym co najmniej przed wszystkimi atakami z listy OWASP Top 10, takimi jak:

a) SQL Injection (SQLi) i NoSQL Injection.
b) Cross-Site Scripting (XSS).
c) Cross-Site Request Forgery (CSRF).
d) Iniekcje poleceń (Command Injection).
e) Ataki na logikę aplikacji.
f) Ataki typu DoS/DDoS na warstwę aplikacyjną (np. HTTP Flood).

1.1.2. Modele bezpieczeństwa: WAF musi wspierać co najmniej negatywny model bezpieczeństwa (blokowanie znanego złośliwego ruchu na podstawie sygnatur).

1.1.3. Zarządzanie regułami i sygnaturami:

a) Oprogramowanie musi umożliwiać elastyczne zarządzanie regułami bezpieczeństwa, w tym ich aktywację w trybie ręcznym oraz automatycznym.
b) Musi posiadać funkcję trybu nauki (learning model), która automatycznie analizuje ruch i sugeruje reguły polityki bezpieczeństwa.

1.1.4. Logowanie i raportowanie: Moduł WAF musi zapewniać szczegółowe logowanie wszystkich zdarzeń bezpieczeństwa, w tym blokowanych żądań i wykrytych anomalii. Musi także oferować predefiniowane raporty zgodności (np. dla PCI DSS) oraz możliwość tworzenia raportów niestandardowych.

1.1.5. Ochrona przed botami: Oprogramowanie musi oferować mechanizmy do identyfikacji i blokowania złośliwego ruchu generowanego przez boty, w tym scrapery i narzędzia do skanowania podatności.

1.2. Architektura Wysokiej Dostępności (High Availability - HA)

1.2.1. Oprogramowanie musi być dostarczone w formie klastra wysokiej dostępności (co najmniej dwie instancje).

1.2.2. Oprogramowanie musi gwarantować ciągłość działania poprzez mechanizm Stateful Failover, zapewniając bezprzerwowe utrzymanie sesji użytkowników w przypadku awarii.

1.3. Wymagania Wydajnościowe (dla pojedynczej instancji)

1.3.1. Każda z instancji klastra musi zapewniać wydajność na poziomie co najmniej:
a) 1 Gbps przepustowości dla równoważenia obciążenia.
b) 3 000 000 jednoczesnych połączeń w warstwie L4.
c) 1000 nowych transakcji na sekundę (SSL TPS).

1.4. Dodatkowe Funkcjonalności Bezpieczeństwa

1.4.1. Oprogramowanie musi posiadać wbudowany system wykrywania i zapobiegania włamaniom (IPS) dla warstwy 7 z obsługą reguł VRT SNORT.

1.4.2. Produkt musi posiadać zaimplementowany moduł autoryzacji z obsługą Single Sign On (SSO), uwierzytelniania wieloskładnikowego (Two Factor Authentication) oraz integracją z Active Directory, Radius i RSA SecurID.

1.5. Forma Dostarczenia i Wirtualizacja

1.5.1. Każda instancja musi być dostarczona jako wirtualne urządzenie (virtual appliance), kompatybilne z platformami wirtualizacyjnymi takimi jak VMware (OVF) lub, Microsoft HYPER-V.

1.6. Zaawansowane Zarządzanie Ruchem i Sesjami

1.6.1. Oprogramowanie musi posiadać funkcjonalność zaawansowanego zarządzania ruchem, oferując szeroki wachlarz metod równoważenia, w tym Round Robin, Least Connection oraz Layer 7 Content Switching.

1.6.2. Oprogramowanie musi umożliwiać **przełączanie ruchu na podstawie treści (Content Switching)**, włączając w to możliwość modyfikacji nagłówków i adresów URL.

1.6.3. Musi zostać zapewniona funkcjonalność **trwałości sesji (Session Persistence)**.

1.7. Obsługa Ruchu Szyfrowanego (SSL/TLS)

1.7.1. Oprogramowanie musi posiadać funkcjonalność **akceleracji i odciążania serwerów z obsługi SSL (SSL offloading)** przy wsparciu dla kluczy 2048-bit i co najmniej 256 certyfikatów SSL.

1.8. Funkcje Sieciowe, Skalowalność i Odporność na Awarie

1.8.1. Oprogramowanie musi posiadać funkcjonalność **Global Server Load Balancing (GSLB)** dla zapewnienia przełączania awaryjnego (failover) pomiędzy centrami danych.

1.8.2. Oprogramowanie musi umożliwiać zdefiniowanie do **1000 wirtualnych serwisów (VIP)**.

1.9. Usługa Wdrożenia i Konfiguracji

1.9.1. W ramach zamówienia Wykonawca musi zapewnić kompletną usługę wdrożenia i konfiguracji dostarczonego klastra HA w środowisku wirtualizacyjnym Zamawiającego. Na realizację usługi musi zostać przeznaczone co najmniej **16 roboczogodzin (2 dni robocze x 8 godzin)** pracy inżyniera, posiadającego certyfikat wystawiony przez producenta oferowanego Oprogramowania.

1.9.2. Podczas usługi wdrożenia muszą zostać wykonane co najmniej następujące czynności:

a) **Instalacja:** Uruchomienie dwóch instancji wirtualnych urządzeń w środowisku Zamawiającego.
b) **Konfiguracja sieciowa:** Podstawowa konfiguracja interfejsów sieciowych, adresacji IP, VLAN oraz routingu w celu integracji z siecią Zamawiającego.
c) **Uruchomienie klastra HA:** Skonfigurowanie klastra wysokiej dostępności w trybie Active/Hot-Standby, w tym mechanizmów synchronizacji i komunikacji (heartbeat).
d) **Testy przełączenia awaryjnego:** Przeprowadzenie i weryfikacja poprawności działania mechanizmu failover w celu potwierdzenia bezprzerwowej pracy usług.
e) **Konfiguracja usług:** Utworzenie i skonfigurowanie co najmniej jednej usługi wirtualnej (VIP) wraz z pulą serwerów rzeczywistych (backend) i odpowiednimi mechanizmami badania ich dostępności (health checks).
f) **Podstawowa konfiguracja bezpieczeństwa:** Wdrożenie certyfikatu SSL, aktywacja reguł WAF oraz konfiguracja dostępu administracyjnego.

1.10. Szkolenie Techniczne dla Administratorów

1.10.1. Wykonawca jest zobowiązany do przeprowadzenia dedykowanego szkolenia technicznego dla 7 administratorów Zamawiającego w wymiarze **co najmniej 5 godzin**.

1.10.2. Szkolenie musi zostać przeprowadzone przez inżyniera, posiadającego certyfikat wystawiony przez producenta oferowanego Oprogramowania. i obejmować co najmniej następujące zagadnienia:
a) Podstawy równoważenia obciążenia.
b) Konfiguracja sieci w ramach rozwiązania.
c) Zarządzanie klastrem wysokiej dostępności (HA).
d) Tworzenie i konfiguracja usług wirtualnych.
e) Zarządzanie certyfikatami i zabezpieczeniami (SSL/TLS).
f) Praktyczne wykorzystanie modułów WAF i autoryzacji (ESP).
g) Konfiguracja opcji rejestrowania zdarzeń (logowania) i monitoringu.
h) Podstawowe metody rozwiązywania problemów (troubleshooting).

1.11. Zarządzanie, Monitoring i Wymagania Ogólne

1.11.1. Oprogramowanie musi oferować **narzędzie do centralnego zarządzania klastrem**.

1.11.2. Oprogramowanie musi zapewnić automatyczną aktualizację sygnatur bezpieczeństwa, zasilany przez renomowane centrum badań nad zagrożeniami, w celu zapewnienia ochrony przed nowymi i ewoluującymi atakami (zero-day).

2. 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 muszę zostać zaprojektowane w sposób minimalizujący negatywny wpływ na środowisko naturalne.