KOMENDA GŁÓWNA POLICJI
BIURO FINANSÓW
WYDZIAŁ ZAMÓWIEŃ PUBLICZNYCH i FUNDUSZY POMOCOWYCH

ul. Domaniewska 36/38; 02-672 Warszawa; tel. 22 60 120 44; fax 22 60 118 57
zamowieniakgp@policja.gov.pl

Warszawa, dnia 08 .01.2019 r.

L.dz. P25-199...../19

Uczestnicy postępowania

Dot. postępowania prowadzonego w trybie przetargu nieograniczonego pn. „Rozbudowa systemu bezpieczeństwa poczty elektronicznej", sprawa nr 332/BŁiI/18/RG/PMP

Działając na podstawie art. 38 ust. 2 oraz ust. 4 ustawy Prawo zamówień publicznych (Dz. U. z 2018 r. poz. 1986) Zamawiający przekazuje odpowiedzi na pytania oraz informację o zmianie SIWZ:

Pytanie nr 1

Wyspecyfikowane przez Zamawiającego rozwiązanie ochrony poczty (ESA Inbound Essentials SW Bundle (AS, AV, OF) License (ESA-ESI-LIC=) oraz Inbound Essential Bundle (AS+AV+OF) 3YR Lic, 100k-249999 Users (ESA-ESI-3Y-S12)) to rozwiązanie subskrypcyjne na okres 36-miesięcy, którego elementem jest również wsparcie techniczne producenta. Podobne warunki dotyczą też innych dostawców tego typu systemów. W związku z tym prosimy o:

1.1. Połączenie czasu trwania subskrypcji na rozwiązanie z okresem gwarancji dla systemu (np. 24-miesiące lub 36-miesięcy).

1.2. Uzależnienia punktacji dodatkowej w ramach systemu oceny ofert od zaoferowania subskrypcji i gwarancji na okres dłuższy niż 24-miesiące. Jednocześnie zwracamy uwagę, że koszt rozwiązania 24-miesięcznego/36-miesięcznego/48-miesięcznego może być znacząco różny i zwłaszcza dla wariantu 48-miesięcznego przekraczać założony budżet.

Odpowiedź

Zamawiający wymaga dostarczenia rozwiązania ze wsparciem producenta licencji, wynoszącym **36 miesięcy**. Długość okresu gwarancji udzielanej przez Wykonawcę zależy od treści oferty Wykonawcy.

Jednocześnie Zamawiający dokonuje modyfikacji SIWZ:

1) Rozdział XIV SIWZ otrzymuje brzmienie:

XIV. OPIS KRYTERIÓW Z PODANIEM ICH ZNACZENIA I SPOSOBU OCENY OFERT:

W odniesieniu do Wykonawców, którzy spełnią warunki udziału w postępowaniu o udzielenie zamówienia publicznego Zamawiający dokona oceny ofert nie odrzuconych na podstawie poniższych kryteriów.

Kryteria oceny ofert i ich znaczenie:

Lp.	Nazwa kryterium	Waga	Współczynnik do wyznaczenia liczby punktów uzyskanych przez Wykonawcę	Sposób oceny
1.	K1 – Cena oferty brutto	60 %	60	Wg wzoru
2	K2 - Okres gwarancji	40 %	40	Wg opisu

Sposób obliczenia punktów w odniesieniu do kryterium „K1 - Cena oferty brutto":

K1 – waga 60 % (maksymalnie Wykonawca może otrzymać 60 punktów)

Cena wyższa od ceny najniższej oceniona zostanie w następujący sposób:

$$K1 = \frac{\text{cena ofertowa minimalna}}{\text{cena ofertowa badana}} \times 60$$

Sposób obliczenia punktów w odniesieniu do kryterium: „K2 – Okres gwarancji":

K2 – waga 40 % (maksymalnie Wykonawca może otrzymać 40 punktów)

Uwaga: Minimalny okres gwarancji, o której mowa w par. 7 projektu umowy (Załącznik nr 3 do SIWZ) wynosi 24 miesiące.

Punkty w ramach ww. kryterium zostaną przyznane w następujący sposób:

- Wykonawca zaoferuje gwarancję na okres 24 miesięcy – 0 punktów,
- Wykonawca zaoferuje gwarancję na okres 36 miesięcy – 40 punktów.

Uwaga:

Długość okresu gwarancji musi zostać określona w pełnych miesiącach.

W przypadku gdy Wykonawca w formularzu ofertowym:

- nie wpisze żadnego okresu gwarancji Zamawiający przyjmie, że Wykonawca oferuje gwarancję na okres 24 miesięcy i przyzna 0 punktów,
- wpisze okres gwarancji w niepełnych miesiącach, Zamawiający do obliczeń w zakresie kryterium *Okres gwarancji* przyjmie okres dokonując zaokrąglenia w dół,
- w przypadku gdy Wykonawca w formularzu ofertowym wpisze okres gwarancji krótszy niż 24 miesiące, Zamawiający odrzuci ofertę, jako niezgodną z SIWZ.

Zasady wyboru oferty i udzielenia zamówienia:

Za najwyżej ocenioną zostanie uznana oferta, która uzyska najwyższą łączna liczbę punktów we wszystkich kryteriach zgodnie ze wzorem:

K = K1 + K2

2) Załącznik nr 2 do SIWZ otrzymuje brzmienie:

Załącznik nr 2 do SIWZ
spr. nr 332/BŁiI/18/RG/PMP

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest „Zakup rozbudowy systemu bezpieczeństwa poczty elektronicznej". Instalacja, konfiguracja i uruchomienie przez Wykonawcę oprogramowania. Dostarczenie Zamawiającemu licencji, dokumentacji oraz realizacja warsztatów szkoleniowych:

1. **ESA Inbound Essentials SW Bundle (AS, AV, OF) License (ESA-ESI-LIC=).**
2. **Inbound Essentials Bundle (AS+AV+OF) 3YR Lic,100K-249999Users (ESA-ESI-3Y-S12).**

lub równoważne w zakresie pkt 1 oraz pkt 2 spełniające n/w wymagania:

1) Ogólne wymagania systemu:

a) Zamawiający oczekuje dostawy całościowego rozwiązania ochrony poczty elektronicznej, które docelowo musi realizować następujące funkcje:

- ochronę przed szkodliwą treścią (m.in. malware, wirusy etc.);
- ochronę przed spamem;
- filtrowanie treści przesyłanej w poczcie elektronicznej (w tym załączniki);

b) Rozwiązanie musi umożliwiać kontrolę protokołu SMTP w tym szyfrowane wersje tego protokołu: SSL i TLS;

c) Rozwiązanie musi zapewniać filtrowanie poczty przychodzącej i wychodzącej, przy czym musi istnieć możliwość przypisana odrębnych polityk dla każdego z kierunków przesyłania poczty elektronicznej;

d) Rozwiązanie musi zapewniać ochronę dla komunikacji z wykorzystaniem protokołu IPv4 i IPv6;

2) Wymagania w zakresie architektury systemu:

a) Rozwiązanie musi posiadać funkcjonalność MTA (Mail Transfer Agent) pracującym w trybie bramy dla przychodzącego i wychodzącego ruchu SMTP;

b) Rozwiązanie musi umożliwiać tworzenie klastrów w trybie active-active z rozkładem obciążenia;

c) Rozwiązanie musi wspierać protokoły SMTP, ESMTP, Secure SMTP over TLS, jako protokoły Mail Injection i Mail Delivery;

d) Rozwiązanie musi posiadać specjalnie zaprojektowany mechanizm do obsługi I/O, zoptymalizowany do obsługi poczty elektronicznej;

e) Konfiguracja Systemu musi być możliwa przez:

- Interfejs Web: HTTP i HTTPS;

- CLI: przez SSH i telnet;

f) Rozwiązanie musi wspierać następujące mechanizmy kryptograficzne:

- TLS: 56-bit DES, 168-bit 3DES, 128-bit RC4, 128-bit AES i 256-bit-AES;
- DomainKeys Signing: 512-, 768-, 1024-, 1536- i 2048-bit RSA;

3) Wymagania w zakresie definiowania polityk:

a) System zarządzania politykami musi umożliwiać wielokrotne wykorzystywanie w regułach predefiniowanych elementów takich jak filtry i akcje;

b) Rozwiązanie musi umożliwiać definiowanie co najmniej następujących akcji (w ramach polityki):

- dostarczenie wiadomości z wykonaniem dodatkowych akcji:
  - zmodyfikowanie tematu przesyłki;
  - usunięcie i/lub dodanie nagłówka X-header;
  - wysłanie kopii wiadomości pod wskazany adres lub adresy email
- zablokowanie wiadomości;
- zapisanie wiadomości do wskazanej kolejki;
- wysłanie powiadomienia;
- przekierowanie wiadomości do kwarantanny;

c) Rozwiązanie musi umożliwiać budowanie polityk i wyjątków od polityk, obejmujących wszystkie funkcjonalności produktu, niezależnie dla ruchu wychodzącego i przychodzącego z zastosowaniem co najmniej:

- domen email;
- obiektów z Microsoft AD;
- adresów email pojedynczych użytkowników;
- adresów IP serwerów mailowych;

d) Rozwiązanie musi umożliwiać tworzenie odrębnych polityk i wyjątków dla różnych użytkowników;

4) Wymagania w zakresie ochrony antyspamowej:

a) Rozwiązanie powinno posiadać rozbudowane narzędzia zapobiegania przesyłaniu SPAM do serwera pocztowego. W tym celu system musi zapewniać mechanizmy ochrony oparte co najmniej o:

- Sygnatury
- Słowniki
- Heurystykę, dla której musi być możliwa regulacja czułości (kontrola ilości False-Positives)

b) Rozwiązanie musi posiadać wbudowane mechanizmy wykrywania wiadomości komercyjnych typu „Newsletters" i umożliwiać traktowanie tych wiadomości w zależności od ustalonej polityki organizacji jako SPAM lub jako wiadomość dopuszczona

c) Rozwiązanie musi zapewnić opcję definiowania wyjątków od stosowanych polityk

d) Mechanizm antyspamowy musi być realizowany dwufazowo.

- Pierwsza faza musi opierać się na sprawdzeniu reputacji adresu IP nadawcy w ogólnoświatowej bazie reputacji, ktora musi posiadać nastepujące parametry:

- Musi otrzymywać dane z co najmniej 100.000 źródeł danych z całego świata;
- Musi analizować co najmniej 150 parametrów dotyczących ruchu poczty elektronicznej i protokołu WWW (w tym co najmniej 90 dla poczty);
- Musi zwracać wynik reputacji dla adresu IP w skali co najmniej 20-stopniowej czyli np. od -10 do 10;
- System musi zwracać rezultat reputacji jedynie na podstawie zbieranych danych, nie dopuszczając jednorazowych interwencji ze strony wysyłających pocztę mających na celu manualne podwyższenie ich reputacji;
- System musi umożliwiać wykorzystanie, co najmniej dwóch systemów badania reputacji nadawców dla poczty przychodzącej. Jeden z nich oparty o publiczny serwis Real-Time Blackhole List (RBL), drugi musi być systemem własnym producenta zaimplementowanym w rozwiązaniu;

– Druga faza ma nastąpić jeżeli wiadomość przejdzie pomyślnie fazę pierwszą i musi opierać się na silniku antyspamowym, korzystającym z reguł otrzymywanych od producenta.

– Reguły muszą być tworzone dynamicznie na podstawie informacji z co najmniej trzech źródeł:

- ogólnoświatowej bazy danych reputacji o parametrach jak w fazie pierwszej,
- informacji zwrotnych od użytkowników proponowanego rozwiązania
- informacji od dedykowanych analityków bezpieczeństwa pracujących 24h na dobę, 7 dni w tygodniu, 365 dni w roku dla producenta proponowanego rozwiązania.

– Reguły muszą weryfikować informacje na temat adresów IP pojawiających się w mailach jako linki do stron, strukturę wiadomości, sposób w jaki została wysłana, treść wiadomości i reputację nadawcy.

– Reguły powinny być uaktualniane, automatycznie, nie rzadziej niż co 5 minut przez internet.

e) Rozwiązanie musi posiadać możliwość skorzystania z funkcji reverse DNS lookup do określenia nazwy domeny dla adresu IP nadawcy wiadomości przychodzącej, wykonanie sprawdzenia, oraz odrzucenie połączenia w przypadku:

– braku rekordu PTR w DNS

– niezgodności nazwy domeny przesłanej w komunikacie SMTP HELO/EHLO z nazwą domeny w rekordzie DNS,

– niezgodności rekordu reverse DNS (PTR) z rekordem forward DNS (A)

f) Rozwiązanie musi umożliwiać weryfikację nadawcy wiadomości w oparciu o mechanizm SPF (Sender Policy Framework). System powinien umożliwiać co najmniej:

– odrzucenie lub przyjęcie wiadomości, jeżeli rekord SPF nie istnieje

– odrzucenie wiadomości, jeżeli rekord SPF nie pasuje do domeny nadawcy

g) Rozwiązanie musi umożliwiać:

– monitorowanie i ograniczanie ilości połączeń z jednego adresu IP w określonym przedziale czasu.

- Musi zapewniać opcję definicji przedziału czasowego
- Musi zapewniać opcję ograniczenia maksymalnej ilości połączeń i wiadomości.

– ograniczanie maksymalnej liczby wiadomości przekazywanych za pomocą pojedynczego połączenia SMTP

– wskazanie timeout'u dla niewykorzystywanego połączenia

h) Rozwiązanie musi pozwalać na blokowanie na określony czas przyjmowania poczty z adresów IP, dla których odnotowano wiadomości zawierające zdefiniowaną liczbę niewłaściwych adresatów z chronionej domeny.

5) Wymagania w zakresie ochrony antywirusowej:

a) Rozwiązanie musi zapewniać blokowanie złośliwej treści:

- z wykorzystaniem tradycyjnego skanowania antywirusowego opartego o co najmniej dwa komercyjne silniki antywirusowe oraz bazy sygnatur kodów złośliwych
- z wykorzystaniem zaawansowanych technik wykrywania zagrożeń jak metody oparte o heurystykę i analizy w czasie rzeczywistym
- musi zapewniać możliwość blokowania niebezpiecznych treści typu ActiveX, Javascript lub VB script.
- musi zapewniać mechanizmy reputacji i sandboxingu plików dla sprawdzenia informacji o przesyłanych obiektach w chmurze w celu wykrywania i blokowania zagrożeń
- System musi umożliwiać definiowanie wyjątków od stosowanych polityk,

b) Silniki antywirusowe muszą korzystać z następujących metod skanowania wiadomości:

- Dopasowanie wzorców binarnych do sygnatur antywirusowych
- Analiza heurystyczna
- Emulacja uruchomienia kodu (w celu zapobiegania infekcji wirusami polimorficznymi)

c) Mechanizm musi mieć do dyspozycji oddzielną od przeznaczonej dla spamu, kwarantannę, do której dostęp ma tylko administrator.

d) Rozwiązanie musi zapewniać mechanizmy dynamicznej ochrony przed epidemią złośliwego kodu:

- Mechanizm antywirusowy musi posiadać technologię umożliwiającą automatyczną kwarantannę wiadomości, które pomimo że nie są wskazane przez powyższe metody skanowania (z powodu np. braku odpowiednich sygnatur antywirusowych), mogą jednak zawierać złośliwy kod.
- Informacje o takim podejrzeniu powinny być wysyłane przez globalną bazę reputacji, o parametrach opisanych w wymogach modułu antyspamowego.
- Podejrzane wiadomości powinny pozostać w kwarantannie, aż do wypuszczenia przez producentów silników antywirusowych odpowiednich sygnatur i automatycznie wypuszczane i skanowane ponownie po ściągnięciu odpowiednich sygnatur.

6) Wymagania w zakresie ochrony przed złośliwym oprogramowaniem:

a) Rozwiązanie musi zapewniać mechanizmy zaawansowanej ochrony antimalware obejmujące:

- Sprawdzenie reputacji dla plików przesyłanych przez urządzenie
- Kontrolę przesyłanych plików przez mechanizm sandboxingu w chmurze
- Monitorowanie wsteczne dla plików już przesłanych

b) Kontrola reputacji dla plików musi odbywać się w ogólnoświatowej bazie reputacji

c) Kontrola reputacji musi odbywać się na podstawie unikatowych metadanych własnościowych pliku, nie jest dopuszczalne, aby sprawdzenie reputacyjne wymuszało przesłanie pliku na zewnątrz systemu kontroli poczty.

d) Funkcja sandboxingu dla plików przesyłanych pocztą elektroniczną musi być wbudowana w system ochrony poczty, nie jest dopuszczalne stosowanie zewnętrznych systemów firm trzecich.

e) Funkcja monitorowania wstecznego musi umożliwiać informowanie administratora o zmianie decyzji dotyczących plików uprzednio przesłanych przez system. W szczególności dotyczy to sytuacji, gdy we wskazanym pliku wykryto złośliwy kod.

7) Wymagania w zakresie filtrowania i kontroli treści:

a) Rozwiązanie musi umożliwiać kontrolę treści wiadomości co najmniej w zakresie:

- słowa kluczowe
- słowniki
- wyrażenia regularne
- typy załączników

b) Kontrola musi obejmować co najmniej następujące elementy wiadomości,

- tytuł,
- treść,
- nagłówki,
- adres nadawcy
- adres odbiorcy

c) Proponowane rozwiązanie musi posiadać mechanizmy analizy i filtrowania oraz zarządzania treścią wiadomości poczty elektronicznej, zarówno treści samej wiadomości jak i jej załączników.

d) Mechanizm musi mieć możliwość zdefiniowania polityki zarządzania treścią wiadomości w oparciu o wynik reputacji pobrany z bazy reputacji o parametrach opisanych w module antyspamowym.

e) Mechanizm musi mieć możliwość zdefiniowania polityki zarządzania treścią wiadomości w oparciu o wynik uwierzytelnienia DKIM, funkcjonalności opisanej w wymaganiach dotyczących zastosowania kryptografii w proponowanym rozwiązaniu

f) Mechanizm musi mieć możliwość filtrowania treści za pomocą integracji z zewnętrznymi słownikami.

g) Rozwiązanie musi umożliwiać zarządzanie kolejkami (folderami) dla blokowanych wiadomości w zakresie zarządzania predefiniowanymi oraz tworzenia nowych.

h) Rozwiązanie musi zapewniać kwarantannę dla zablokowanych wiadomości. Dla kolejki kwarantanny musi być możliwe zdefiniowanie jej maksymalnej wielkości oraz czasu, po którym wiadomości będą usuwane

8) Wymagania w zakresie kryptografia:

a) Rozwiązanie musi posiadać mechanizmy oznaczania poczty wychodzącej (Bounce Address Tag Validation (BATV)) oraz weryfikacji tego oznaczenia w przypadku otrzymania wiadomości odbitej od odbiorcy (tzw. Bounce) w celu ochrony przed atakami typu „misdirected bounce spam"

b) Rozwiązanie musi obsługiwać standard DKIM (Domain Keys Identified Messages) używany w celu uwierzytelnienia poczty, za pomocą szyfrowania asymetrycznego.

c) Rozwiązanie musi umożliwiać opcjonalnie, oddzielnie licencjonowane, szyfrowanie symetryczne poczty dla wybranych wiadomości, wykonywane bez potrzeby jakiejkolowiek ingerencji w klienta pocztowego oraz bez potrzeby implementacji PKI. Rozwiązanie powinno udostępniać szyfrowanie za pomocą algorytmów AES oraz RC4.

9) Wymagania w zakresie modułu raportującego i zarządzającego:

1. Konfiguracja Systemu musi być możliwa przez:

- Interfejs Web: HTTP i HTTPS

- CLI: przez SSH i telnet

2. Rozwiązanie musi być wyposażone w system raportujący, umożliwiający:
   - Generowanie predefiniowanych oraz własnych raportów na żądanie oraz zgodnie z harmonogramem.
   - Harmonogram powinien umożliwiać generowanie raportów codziennie, co tydzień lub co miesiąc.
   - Powinno być możliwe dostarczanie raportów w postaci plików pdf i csv.
   - Powinno być możliwe dostosowanie tematu i treści automatycznie wysyłanego maila zawierającego generowane raporty.
3. Zarządzanie, przeglądanie aktywności użytkowników oraz raportowanie powinny być dostępne przez zintegrowaną webową konsolę administracyjną
4. Dostęp do webowej konsoli zarządzającej powinien odbywać się przy użyciu bezpiecznego połączenia HTTPS.
5. Konsola zarządzająca powinna zawierać ekran przedstawiający wykres sumarycznej aktywności z ostatnich 24 godzin oraz podstawowe statystki.
6. Rozwiązanie powinno udostępniać mechanizm pozwalający na przeglądanie przez chronionych użytkowników wiadomości umieszczonych w kwarantannie, umożliwiając im również zwolnienie wybranych wiadomości z kwarantanny

10) Wymagania w zakresie licencji:

a) Proponowane rozwiązanie musi być zaoferowane z możliwością instalacji systemu na nieograniczonej liczbie maszyn wirtualnych

b) Proponowane rozwiązanie powinno mieć licencje na okres **36 miesięcy** na następujące funkcjonalności: MTA, DKIM, BATV i filtrowania treści.

c) Proponowane rozwiązanie powinno posiadać licencje dla ochrony 100000 skrzynek pocztowych na **36 miesięcy** (z możliwością przedłużenia) na następujące funkcjonalności:
   - Antyspam,
   - Antywirus z wykorzystaniem jednego silnika komercyjnego
   - Antiwirus z obsługą ochrony przed epidemią złośliwego kodu

3. Instalacja, konfiguracja i uruchomienie w/w środowiska wg. zakresu:

a) wizja lokalna w miejscu instalacji,

b) projekt techniczny zawierający analizę infrastruktury fizycznej i logicznej, przygotowanie kompletnej dokumentacji implementacyjnej,

c) instalacja w siedzibach Zamawiającego,

d) Konfiguracja i instalacja oprogramowania zgodnie z projektem,

e) przygotowanie scenariuszy i przeprowadzenie testów akceptacyjnych,

f) przygotowanie dokumentacji projektowej, eksploatacyjnej, powykonawczej.

4. Warsztaty szkoleniowe z zarządzania i administracji systemem bezpieczeństwa poczty elektronicznej, przeprowadzone dla 8 osób.

5. Wsparcie producenta licencji na okres 36 miesięcy.

Pytanie nr 2

Dotyczy punktu 10.b sekcji Wymagania w zakresie licencji.

Prosimy o jego wykreślenie – dostarczane rozwiązanie (i opisane wzorcowe) jest realizowane w modelu subskrypcyjnym zatem oferent nie może zapewnić dostawy licencji na czas nieokreślony.

Odpowiedź

Zamawiający dokonuje modyfikacji zapisów Załącznika nr 2 do SIWZ. Punkt 10.b Załącznika nr 2 do SIWZ otrzymuje brzmienie:

*b) Proponowane rozwiązanie powinno mieć licencje na okres **36 miesięcy** na następujące funkcjonalności: MTA, DKIM, BATV i filtrowania treści.*

Pytanie nr 3

Dotyczy punktu 10.c sekcji Wymagania w zakresie licencji.

Prosimy o wyjaśnienie czy nie nastąpiła omyłka w wymaganiu dotyczącym okresu na jaki należy dostarczyć wymagane funkcjonalności. W punkcie 10.c jest napisane:" *na dwa lata*", natomiast w punkcie 5 Zamawiający wymaga wsparcia producenta licencji na 36 miesięcy. Prosimy o ujednolicenie zapisu.

Odpowiedź

Zamawiający dokonuje modyfikacji zapisów Załącznika nr 2 do SIWZ. Punkt 10.c Załącznika nr 2 do SIWZ otrzymuje brzmienie:

*c) Proponowane rozwiązanie powinno posiadać licencje dla ochrony 100000 skrzynek pocztowych na **36 miesięcy** (z możliwością przedłużenia) na następujące funkcjonalności:*

- *Antyspam,*
- *Antywirus z wykorzystaniem jednego silnika komercyjnego*
- *Antiwirus z obsługą ochrony przed epidemią złośliwego kodu*

Pytanie nr 4

Dotyczy §11 Licencje (projekt Umowy).

Wyspecyfikowane przez Zamawiającego rozwiązanie ochrony poczty (ESA Inbound Essentials SW Bundle (AS, AV, OF) License (ESA-ESI-LIC=) oraz Inbound Essential Bundle (AS+AV+OF) 3YR Lic, 100k-249999 Users (ESA-ESI-3Y-S12)) to rozwiązanie subskrypcyjne.

Prosimy o dostosowanie zapisów projektu umowy, w sposób umożliwiający zaoferowanie wyspecyfikowanych produktów w ich modelu subskrypcyjnym. Aktualnie §11 (Licencje) m.in. w pkt. 4 odnosi się wprost do licencji stałych (permanent) poprzez zapis:

„...niewyłączną licencję nieograniczoną w czasie...", jak również w §11. punktach 6, 7.

Odpowiedź

Zamawiający dokonuje modyfikacji Załącznika nr 3 do SIWZ. § 11 ust. 4 projektu umowy otrzymuje brzmienie:

4. *Z chwilą podpisania protokołu odbioru Przedmiotu umowy, w ramach wynagrodzenia wskazanego w § 6 ust. 1 Umowy Wykonawca zapewnia Zamawiającemu licencję* ***na czas określony 36 miesięcy****, na dostarczone oprogramowanie, uprawniającą Zamawiającego do używania oprogramowania zgodnie z jego przeznaczeniem lub celem dla jakiego jest kupowany, oraz przekaże Zamawiającemu wszelką dokumentację i środki potrzebne do korzystania i rozporządzania nabytym przez Zamawiającego oprogramowaniem na następujących polach eksploatacji:*
   a. *prawo do korzystania z wszystkich funkcjonalności Oprogramowania, do którego zostały dostarczone w ramach Umowy Licencje, w dowolny sposób w liczbie kopii/ stanowisk/ serwerów/ użytkowników charakterystycznej dla dostarczonych Licencji do Oprogramowania;*
   b. *prawo do instalowania Oprogramowania, do którego zostały dostarczone w ramach Umowy Licencje, w liczbie kopii/ stanowisk/ serwerów/ użytkowników charakterystycznej dla dostarczonych Licencji do Oprogramowania;*
   c. *prawo do instalowania wszelkich poprawek i uaktualnień opublikowanych na stronach producenta Oprogramowania oraz polach eksploatacji określonych w opublikowanych przez producenta warunkach licencyjnych;*
   d. *instalowanie i deinstalowanie Oprogramowania pod warunkiem zachowania liczby udzielonych Licencji;*
   e. *prawo do utrwalania przez Zamawiającego Oprogramowania, do którego zostały dostarczone w ramach Umowy Licencje, na nośnikach.*

Pytanie nr 5

W ramach opisywanych warunków równoważności pojawiają się punkty wymagające dodatkowych - w stosunku do wyspecyfikowanych przez Zamawiającego - licencji. Prosimy o potwierdzenie, że funkcje te mają być spełniane przez oferowane rozwiązanie – ale dostarczenie licencji do nich nie jest wymagane na etapie postępowania, a możliwe do dokupienia przez Zamawiającego w przyszłości. Dotyczy to w szczególności punktów: 5a (drugi komercyjny silnik antywirusowy), pkt. 6 (zaawansowana ochrona antymalware), pkt. 7 (moduł filtracji treści – w zakresie DLP), pkt. 8 (kryptografia).

Odpowiedź

Zamawiający oczekuje dostarczenia wyłącznie licencji wymienionych w punkcie 10c. Dostarczone rozwiązanie musi posiadać wymienione w parametrach równoważności funkcjonalności, a ich uruchomienie ma wymagać wyłącznie zakupienia niezbędnej dodatkowych licencji/subskrypcji.

Pytanie nr 6

Prosimy o potwierdzenie, że opisywane w pkt. 6a Monitorowanie wsteczne dla plików już przesłanych dotyczy sytuacji, gdzie plik przesyłany pocztą po przejściu przez systemy ochrony antymalware i sandbox, są uznane za „dobre" lub „nieznane" i przesłane do odbiorcy, ale system przechowuje o tych plikach informacje (np. w postaci cache'a hash'y), aby w przypadku zmiany dyspozycji (np. na skutek działania ekspertów bezpieczeństwa producenta, informacji zwrotnych od innych klientów itp.) administrator miał pełną świadomość, kto i kiedy taki plik otrzymał, aby móc łatwo podjąć akcję remediacji.

Odpowiedź

Zamawiający potwierdza, że opisywane w punkcie 6a Monitorowanie wsteczne dla plików już przesłanych dotyczy sytuacji, gdzie plik przesyłany pocztą po przejściu przez systemy ochrony antymalware i sandbox, są uznane za „dobre" lub „nieznane" i przesłane do odbiorcy, ale system przechowuje o tych plikach informacje (np. w postaci cache'a hash'y), aby w przypadku zmiany dyspozycji (np. na skutek działania ekspertów bezpieczeństwa producenta, informacji zwrotnych od innych klientów itp.) administrator miał pełną świadomość, kto i kiedy taki plik otrzymał, aby móc łatwo podjąć akcję remediacji.

Pytanie nr 7

Czy Zamawiający potwierdza, że elementem postępowania jest dostarczenie licencji i posiada odpowiednie zasoby sprzętowe do instalacji opisywanego rozwiązania? Prosimy o potwierdzenie, że oferowany system nie może mieć ograniczeń na liczbę instalowanych maszyn wirtualnych (zgodnie z pkt. 10a), aby w razie zwiększania obciążeń systemu (zwiększanie funkcjonalności o dodatkowe komponenty, ilości przesyłanych maili) można było łatwo i bezkosztowo (z punktu widzenia licencji na maszyny wirtualne) rozbudowywać oferowany system.

Odpowiedź

Zamawiający potwierdza, że elementem postępowania jest dostarczenie licencji i posiada odpowiednie zasoby sprzętowe do instalacji opisywanego rozwiązania? Prosimy o potwierdzenie, że oferowany system nie może mieć ograniczeń na liczbę instalowanych maszyn wirtualnych (zgodnie z pkt. 10a), aby w razie zwiększania obciążeń systemu (zwiększanie funkcjonalności o dodatkowe komponenty, ilości przesyłanych maili) można było łatwo i bezkosztowo (z punktu widzenia licencji na maszyny wirtualne) rozbudowywać oferowany system.

Pytanie nr 8

Czy Zamawiający przewiduje wykorzystanie do zarządzania i raportowania rozwiązaniem interfejsów programistycznych (API)? W ramach postępowania nie przewidziano centralnego systemu zarządzania, co powoduje, że API mogłoby znacząco ułatwić wykorzystanie systemu i jego integrację z narzędziami wykorzystywanymi przez Zamawiającego.

Odpowiedź

Tak, Zamawiający oczekuje, że dostarczone rozwiązanie posiada interfejs programistyczny (API) pozwalający na zarządzanie i co najmniej raportowanie bieżących parametrów określających status systemu.

Pytanie nr 9

Dotyczy Warsztatów szkoleniowych.

a. Czy Zamawiający wymaga realizacji autoryzowanych Warsztatów szkoleniowych w certyfikowanym centrum szkoleniowym?

b. Czy Zamawiający uzna realizację Warsztatów szkoleniowych poprzez dostarczenie voucherów na warsztaty z rocznym terminem ich wykorzystania?

c. Czy Zamawiający dopuści przekazania dokumentacji warsztatowej w języku angielskim?

Odpowiedź

a. Zamawiający nie wymaga realizacji szkoleń w autoryzowanym centrum szkoleniowym, natomiast Zamawiający wymaga przeprowadzenia szkoleń przez szkoleniowca posiadającego udokumentowane doświadczenie i wiedzę w zakresie oferowanego produktu na poziomie zaawansowanym.
b. Zamawiający nie dopuszcza voucherów.
c. Zamawiający dopuszcza materiały szkoleniowe w języku angielskim

Pytanie nr 10

Czy Zamawiający dopuszcza zmianę definicji „Czas Usunięcia Awarii" wprowadzenie zapisu, że jest to czas liczony od momentu potwierdzenia przyjęcia zgłoszenia przez Wykonawcę?

Odpowiedź

Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 11

Czy Zamawiający dopuści możliwość wykreślenia § 8 ust. 2b Załącznika nr 3 do SIWZ? Ten ustęp jest powtórzeniem pozostałych kar umownych, bowiem wszystkie pozostałe odnoszą się do niewykonania lub nienależytego wykonania umowy.

Odpowiedź

Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 12

Czy Zamawiający dopuści możliwość zmiany w § 8 ust. 2c, e, f poprzez wprowadzenie odniesienia do zwłoki, zamiast do opóźnienia?

Odpowiedź

Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 13

Czy Zamawiający wyrazi zgodę na usunięcie zapisu § 8 ust. 4 Załącznika nr 3 do SIWZ stanowiącego o możliwości potrącania kar umownych?

Odpowiedź

Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 14

Czy Zamawiający wyrazi zgodę na wprowadzenie zmian do Załącznika nr 3 do SIWZ poprzez wskazanie, że łączna wysokość kar umownych zostaje ograniczona do 20% wynagrodzenia netto?

Odpowiedź

Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 15

Czy Zamawiający wyrazi zgodę na wykreślenie § 8 ust. 6 Załącznika nr 3 do SIWZ?

Odpowiedź

Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 16

Załącznik nr 3 do SIWZ nie ogranicza odpowiedzialności Wykonawcy i nakłada na niego ewentualne ciężary przewyższające możliwe do uzyskania wynagrodzenie oraz wartość realnej szkody Zamawiającego? Czy Zamawiający dopuści zmianę umowy poprzez dodanie postanowienia, z którego wynikało będzie, iż całkowita odpowiedzialność Wykonawcy z tyłu Umowy zostanie ograniczona do wartości 100% wynagrodzenia netto?

Odpowiedź

Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 17

Czy Zamawiający dopuszcza możliwość wyłączenia rękojmi?

Odpowiedź

Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 18

Czy w przypadku odstąpienia określonego w § 10 ust. 1 pkt 2 Załącznika nr 3 do SIWZ Zamawiający dopuszcza wprowadzenie okresu naprawczego 14 dni dla Wykonawcy i zawiadomienia Wykonawcy o zamiarze odstąpienia od Umowy z wyprzedzeniem?

Odpowiedź

Zamawiający podtrzymuje zapisy umowy. Ewentualne odstąpienie od umowy nastąpi zgodnie z obowiązującymi przepisami prawa.

Pytanie nr 19

Czy Zamawiający wyraża zgodę na zastąpienie §11 jednym ustępem który będzie stanowił, że licencje zostają udzielone na zasadach określonych przez producenta?

Odpowiedź

Zamawiający podtrzymuje zapisy SIWZ.

Pytanie nr 20

Czy Zamawiający wyrazi zgodę na wprowadzenie postanowienia, zgodnie z którym prawa autorskie do dokumentacji przejdą na Zamawiającego w dniu zapłaty całości wynagrodzenia?

Odpowiedź

Zamawiający podtrzymuje zapisy SIWZ.

Powyższe wyjaśnienia i zmiana są wiążące dla stron postępowania.

ZASTĘPCA NACZELNIKA
Wydziału Zamówień Publicznych
Komendy Stołecznej Policji
Anna ŁUCHOWSKA

wykonano w 1 egz.:
opr./wyk. R. Gasek
tel. 22 60 115 11