Warszawa, 24 listopada 2020 r.

Samorządowe Kolegium Odwoławcze w Warszawie
Ul. Obozowa 57
01-161 Warszawa
tel. + 48 22 622 49 61-64
fax + 48 22 625 21 66

Zaproszenie do złożenia oferty cenowej nr 13/2020

(dotyczy zamówienia urządzeń służących do kompleksowej ochrony poczty elektronicznej)

I. ZAMAWIAJĄCY

Samorządowe Kolegium Odwoławcze w Warszawie
ul. Obozowa 57, 01-161 Warszawa
NIP: 526-16-56-044

II. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest zakup urządzeń i oprogramowania służących do kompleksowej ochrony poczty elektronicznej
2. Szczegółowy opis przedmiotu zamówienia:

Urządzenie/urządzenia musi być fabrycznie nowe, nieużywane i być wyprodukowane nie wcześniej niż w roku 2020. Na obudowie urządzenia musi być etykieta potwierdzająca datę jego produkcji.

Wymagania ogólne

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:

1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).
3. Tryb serwera pocztowego

Parametry fizyczne systemu antyspamowego

1. System musi być wyposażony w interfejsy:
- 4 porty Gigabit Ethernet RJ-45.
2. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1 TB

.

3. System musi posiadać wbudowany port konsoli szeregowej.
4. Zasilanie z sieci 230V/50Hz.

Funkcja serwera poczty

W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 150 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych.

Funkcje serwera poczty

W tym zakresie dostarczony system musi zapewniać:

1. Obsługę serwisów pocztowych: SMTP, POP3, IMAP.
2. Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, oraz TLS 1.2).
3. Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników.
4. Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, oraz TLS 1.2).
5. Polski interfejs użytkownika przy dostępie przez WebMail.
6. Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP.
7. Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP.

Ogólne funkcje systemu ochrony poczty

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 20 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 28 tys wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
7. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
8. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
9. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
10. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail oraz IMAP.
11. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
12. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
13. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
14. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
15. Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Prevention).

Kontrola antywirusowa i ochrona przed malware

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.

2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
9. Ochronę typu wirus outbrake.

Kontrola antyspamowa

System musi zapewniać poniższe funkcje i metody filtrowania spamu:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.
13. Ochrona typu outbrake.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.

Ochrona przed atakami na usługę poczty

System musi zapewniać poniższe funkcje i metody filtrowania:

1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

Funkcje logowania i raportowania

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.

2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

Funkcje pracy w trybie wysokiej dostępności (HA)
System ochrony poczty musi zapewniać poniższe funkcje:

1. Konfigurację HA w każdym z trybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.

Aktualizacje sygnatur, dostęp do bazy spamu
W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

Zarządzanie
System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 7 lokalnych kont administracyjnych.

Certyfikaty
1. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.

Serwisy i licencje
W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu virus outbrake, usługa sandbox w chmurze, szyfrowanie, DLP oraz archiwizacja na okres 36 miesięcy.

Gwarancja oraz wsparcie
1. System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Rozszerzone wsparcie serwisowe
1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu max. w ciągu

1 dnia roboczego od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 36 miesięcy.

Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent winien przedłożyć dokumenty:

- Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
- Certyfikat ISO 9001 podmiotu serwisującego.

Opisy do wymagań ogólnych

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Wdrożenie

W ramach dostarczonego rozwiązania, Wykonawca przeprowadzi proces migracji poczty z obecnie używanego serwera poczty przez Zamawiającego. Zamawiający przez pierwsze 2 miesiące od wdrożenia, będzie miał do wykorzystania 20h konsultacji, celem zaimplementowania całkowitej konfiguracji dostarczonego rozwiązania.

Szkolenie

W ramach dostarczonego rozwiązania Wykonawca przeprowadzi certyfikowane szkolenie dla min. 1 osoby, które będzie zawierało co najmniej poniższe zagadnienia:

-
zagrożenia związane z pocztą elektroniczną
- tryby pracy urządzenia
- podstawy protokołów pocztowych
- podstawowa konfiguracja urządzenia
- konfiguracja połączenia sieciowego
- konta administracyjne
- logowanie
- generowanie raportów
- obsługa SNMP
- "Chronione" domeny pocztowe
- potwierdzanie odbiorców
- kwarantanna
- zarządzanie pocztą użytkowników
- aliasy pocztowe
- kolejki e-mail
- reguły Access Control
- polityki i profile
- reguły dostarczenia
- polityki w oparciu o IP
- polityki w oparciu o odbiorcę
- metody antyspamowe
- profile i techniki
- tagi X-FEAS
- wskazówki konfiguracyjne
- konfiguracja profili sesji
- reputacja nadawcy/odbiorcy
- sprawdzenie nadawcy
- SMTP - limity
- manipulacja nagłówkami
- moduł antywirusowy

- profile skanowania treści i załączników
- warunki skanowania
- archiwizacja i kwarantanna
- zarządzanie zarchiwizowaną pocztą
- ustawienia użytkownika dot. kwarantanny
- raporty z kwarantanny
- uwierzytelnienie poprzez SMTP
- wsparcie dla PKI
- protokół SMTPS
- protokół SMTP over Transport Layer Security (TLS)
- profil TLS
- S/MIME
- Identity Based Encryption (IBE)
- LDAP
- profile i zapytania LDAP
- weryfikacja odbiorcy i domeny
- aliasy pocztowe
- routing poczty
- struktura danych
- informacje o systemie
- błędy sprzętowe
- kopia zapasowa
- komendy diagnostyczne
- analiza logów
- konfiguracja interfejsów sieciowych
- tryb Bridge oraz Router
- scenariusze wdrożenia
- tryb Configuration Share
- tryb Active-Passive Mode
- konfiguracja klastra
- interfejs Heartbeat
- monitoring klastra
- procedura upgradu
- użytkownicy i grupy użytkowników
- globalna oraz osobista książka adresowa
- kalendarz

3. Zamawiający nie dopuszcza możliwości składania ofert częściowych.
4. Zamawiający nie dopuszcza możliwości powierzenia części lub całości zamówienia podwykonawcom.

III. TERMIN WYKONANIA ZAMÓWIENIA

Termin wykonania przedmiotu zamówienia: do 23.12.2020 r.

IV. OPIS SPOSOBU PRZYGOTOWANIA OFERTY

Oferent powinien stworzyć ofertę na formularzu załączonym do niniejszego zapytania i dołączyć niezbędne dokumenty/oświadczenia wskazane w szczegółowym opisie przedmiotu zamówienia.

Oferta powinna być:
- opatrzona pieczątką firmową,
- posiadać datę sporządzenia,
- zawierać adres lub siedzibę oferenta, numer telefonu, numer NIP,
- podpisana czytelnie przez wykonawcę.

V. MIEJSCE ORAZ TERMIN SKŁADANIA OFERT

1. Oferta powinna być przesłana za pośrednictwem: poczty elektronicznej na adres: s_jamiolkowski@warszawa.sko.gov.pl , faksem na nr: 22 625 21 66, poczty, kuriera lub też dostarczona osobiście na adres:

   Samorządowe Kolegium Odwoławcze w Warszawie
   Ul. Obozowa 57
   01-161 Warszawa

do dnia 03.12.2020 r. do godziny 12.00. wraz z załączoną kserokopią wypisu z rejestru przedsiębiorców lub zaświadczenia z ewidencji działalności gospodarczej, wystawione w dacie nie wcześniejszej niż sześć miesięcy przed datą złożenia oferty.

2. Ocena ofert zostanie dokonana w dniu 03.12.2020 r. a wyniki i wybór najkorzystniejszej oferty zostanie przekazany wszystkim oferentom mailowo oraz ogłoszony na stronie internetowej pod adresem www.bip.warszawa.sko.gov.pl
3. Oferty złożone po terminie nie będą rozpatrywane
4. Oferent może przed upływem terminu składania ofert zmienić lub wycofać swoją ofertę.
5. W toku badania i oceny ofert Zamawiający może żądać od oferentów wyjaśnień dotyczących treści złożonych ofert.

6. Zapytanie ofertowe zamieszczono na stronie: www.bip.warszawa.sko.gov.pl

VI. OCENA OFERT

Zamawiający dokona oceny ważnych ofert na podstawie następujących kryteriów:
1 - Cena 100%

VII. INFORMACJE DOTYCZĄCE WYBORU NAJKORZYSTNIEJSZEJ OFERTY

O wyborze najkorzystniejszej oferty Zamawiający zawiadomi oferentów pisemnie.

VIII. DODATKOWE INFORMACJE

Dodatkowych informacji udziela Sebastian Jamiołkowski pod numerem telefonu 22 622 49 61 wew. 139 oraz adresem email: s_jamiolkowski@warszawa.sko.gov.pl

IX. ZAŁĄCZNIKI

- Wzór formularza ofertowego
- Wzór umowy

KIEROWNIK BIURA
Samorządowego Kolegium Odwoławczego
w Warszawie
Anna Spodobalska

Warszawa, ...

.....
Nazwa bądź imię i nazwisko Oferenta

.....
Adres lub siedziba Oferenta

.....
Kod i miejscowość

.....
NIP

.....
Nr telefonu

OFERTA
(dotyczy Zaproszenia do złożenia oferty cenowej nr 13/2020)

Przedmiot zamówienia	**Nazwa producenta**	**Model / Nazwa produktu**	**Wartość netto**
Zaproponowane rozwiązanie			
		Suma netto	
		Wartość brutto	

.....
Podpis