***Załącznik nr 1A- opis przedmiotu zamówienia dla zakresu nr 2 – Modyfikacja***

Email Security Gateway — opis funkcjonalny

**Wymagania ogólne**

System filtrowania poczty elektronicznej w postaci urządzenia typu *appliance*: Email Security Gateway **wraz z wdrożeniem oraz szkoleniem dla 4 użytkowników.**

**Parametry techniczne**

1. Obudowa typu RACK 19” o wysokości 1U.
2. Minimalna liczba interfejsów sieciowych urządzenia to co najmniej 1 interfejs Gigabit.
3. Urządzenie przeznaczone jest do obsługi 1000 użytkowników.
4. Ilość przestrzeni dyskowej przeznaczonej na kwarantannę to minimum 20GB.
5. Liczba obsługiwanych domen: min. 250
6. Przestrzeń dyskowa logów i bufora wiadomości: nie mniejsza niż 12 GB
7. Kwarantanna działająca w trybie globalnym (adres email przeznaczony do odbioru wiadomości co do których podjęto decyzję o kwarantannie) z obsługą w logu wiadomości
8. Oferowane rozwiązanie musi posiadać Deklarację zgodności CE

**Ochrona przed spamem**

1. Urządzenie ma:
2. zapewniać ochronę zarówno poczty przychodzącej jak i wychodzącej,
3. zapobiegać próbom spoofingu, phisingu i spyware,
4. zabezpieczać przed atakami typu DoS (Denial of Service),
5. zabezpieczać pocztę wychodzącą, w skład której wchodzi ochrona antywirusowa, kontrola ilości wysłanych wiadomości przez użytkownika,
6. zapewniać ochronę przed atakami typu DHA (Directory Harvest Attack).
7. W ramach ważnego serwisu na urządzenie, administrator ma możliwość zainstalowania dostarczonego przez producenta urządzenia skanera antywirusowego dla MS Exchange 2007/2010/2013.
8. Możliwość ustawiania progów na podstawie punktacji przypisanej przez algorytmy modułu antyspamowego dla wiadomości przychodzących, wg której wiadomości mogą być blokowane, przesyłane do kwarantanny lub oznaczane jako spam.
9. Możliwość ustawiania progów na podstawie punktacji przypisanej przez algorytmy modułu antyspamowego dla wiadomości wychodzących, wg której wiadomości mogą być blokowane lub przesyłane do kwarantanny.
10. Analiza odcisku palca wiadomości (fingerprint), pozwalająca na zweryfikowanie wiadomości przychodzącej z bazą odcisków wiadomości zawierających spam, stworzonej przez producenta.
11. Analiza obrazów dołączonych do wiadomości przy pomocy skanera OCR (Optical Character Recognition).
12. Weryfikacja adresów URL zawartych w wiadomości z bazą danych znanych adresów URL zawierających spam. Możliwość blokowania, oznaczania, przenoszenia do kwarantanny takich wiadomości spamowych.
13. Urządzenie ma mieć możliwość korzystania z filtrów Bayesa.
14. Możliwość określania maksymalnej ilości połączeń z danego adresu IP do urządzenia, w zdefiniowanym przez administratora przedziale czasu. Ustawienie dotyczy zarówno poczty wychodzącej jak i przychodzącej.
15. Możliwość określania maksymalnej ilości wysłanych wiadomości od danego nadawcy w zdefiniowanym przez administratora przedziale czasu. Ustawienie dotyczy poczty wychodzącej.
16. Możliwość zdefiniowania adresów email wyłączonych ze sprawdzania maksymalnej ilości wysyłanych wiadomości w zdefiniowanym przez administratora przedziale czasu.
17. Możliwość zdefiniowania adresów email wyłączonych ze sprawdzania maksymalnej ilości wysyłanych wiadomości w zdefiniowanym przez administratora przedziale czasu.
18. Uwierzytelnianie nadawcy wiadomości na podstawie SPF (Sender Policy Framework).
19. Uwierzytelnianie nadawcy wiadomości na podstawie mechanizmu DKIM (Domain Keys).
20. Zapobieganie niepożądanym wiadomościom bounce z wykorzystaniem metody oznaczania nagłówków wiadomości wysyłanych przez urządzenie.
21. Możliwość korzystania z dowolnych zewnętrznych baz RBL.
22. Urządzenie ma zapewniać dostęp do baz reputacyjnych producenta, które zawierają listę znanych spamerów.
23. Możliwość zdefiniowania wykluczeń ze skanowania antyspamowego dla wiadomości wychodzących/przychodzących ze określonego adresu IP lub zakresu adresów IP.
24. Możliwość zdefiniowania akcji dla wiadomości przychodzących w przypadku gdy wiadomości zostały wysłane z określonego adresu IP lub określonej podsieci. Dostępne akcje w tym przypadku to: blokowanie, poddanie kwarantannie lub oznaczenie wiadomości jako spam.
25. Możliwość zdefiniowania białej listy domen, subdomen.
26. Możliwość zdefiniowania czarnej listy domen, subdomen. Wiadomości przychodzące z tych domen/subdomen mogą być blokowane, oznaczone jako spam lub przenoszone do kwarantanny.
27. Możliwość określenia dla jakich domen chronionych przez urządzenie poczta wychodząca będzie szyfrowana przy pomocy protokołu TLS.
28. Możliwość określenia domen chronionych przez urządzenie, dla których poczta wychodząca będzie przekierowana na inny serwer pocztowy.
29. Możliwość określenia dla jakich adresów email poczta wychodząca będzie szyfrowana przy pomocy protokołu TLS.
30. Możliwość określenia adresów email, dla których poczta wychodząca będzie przekierowana na inny serwer pocztowy.
31. Możliwość blokowania wiadomości pochodzących z konkretnego kraju, do wyboru ma być minimum 9 krajów takich jak: Argentyna, Brazylia, Chile, Chiny, Kolumbia, Niemcy, Włochy, Rosja, Turcja.
32. Możliwość tworzenia reguł pozwalających na blokowanie, przesyłanie do kwarantanny lub oznaczenia wiadomości jako spam wiadomości pochodzących z danego hosta.
33. Produkt powinien rozróżniać co najmniej 11 różnych zestawów znaków, różnych narodowości używanych do kodowania wiadomości mailowych. Wiadomości posiadające takie znaki mogą być blokowane, przesłane do kwarantanny lub oznaczone jako spam.
34. Urządzenie ma umożliwiać korzystanie użytkownikom z dodatkowego pluginu do aplikacji Microsoft Outlook.
35. Możliwość uruchomienia SMTP over TLS zarówno dla połączeń wychodzących jak i przychodzących.
36. Możliwość wymuszenia zgodności protokołu SMTP z RFC 821.
37. Możliwość blokowania wiadomości które nie używają FQDN (fully-qualified domain name) w polu ‘From’ adresu.

**Kontrola Treści**

1. Kontrola zawartości załączników po:
2. typie pliku, co najmniej następujące typy: MS Access, MS Excel, MS Word, Adobe PDF, MS PowerPoint, Windows exe, Windows Script. Skaner sprawdza również archiwa pod kątem obecności zdefiniowanych typów pliku,
3. nazwie pliku lub rozszerzenia pliku, definiowane przez administratora,
4. typie MIME pliku, definiowane przez administratora zgodnie ze standardem RFC.
5. Dostępne akcje w przypadku kontroli załączników wiadomości mają być rozdzielone ze względu na pocztę przychodzącą i wychodzącą:
6. poczta przychodząca: blokowanie, przeniesienie do kwarantanny,
7. poczta wychodząca: blokowanie, przeniesienie do kwarantanny, zaszyfrowanie, przekierowanie na inny serwer.
8. Dostępne akcje w przypadku spakowanych, zabezpieczonych hasłem załączników wiadomości mają być rozdzielone ze względu na pocztę przychodzącą i wychodzącą:
9. poczta przychodząca: blokowanie, przeniesienie do kwarantanny,
10. poczta wychodząca: blokowanie, przeniesienie do kwarantanny, zaszyfrowanie, przekierowanie na inny serwer.
11. Możliwość tworzenia reguł, przy pomocy wyrażeń regularnych filtrujących wiadomości po temacie, nagłówku i treści wiadomości. Możliwość tworzenia takich reguł zarówno dla wiadomości przychodzącej jak i wychodzącej. Dostępne akcje mają być rozdzielone ze względu na pocztę przychodzącą i wychodzącą:
12. poczta przychodząca: blokowanie, przeniesienie do kwarantanny, oznaczenie wiadomości, dodanie do białej listy,
13. poczta wychodząca: blokowanie, przeniesienie do kwarantanny, zaszyfrowanie  wiadomości, dodanie do białej listy, przekierowanie na inny serwer.
14. Minimum 4 predefiniowane, stworzone przez producenta reguły poczty wychodzącej, filtrujące wiadomości po temacie, nagłówku i treści wiadomości.

**Ochrona antywirusowa**

1. Urządzenie ma zapewniać skanowanie antywirusowe poczty przychodzącej przy pomocy minimum 3 różnych silników antywirusowych działających jednocześnie.
2. Weryfikacja odcisku wiadomości lub wirusa z bazą danych producenta, jeżeli informacje na temat tej wiadomości lub wirusa nie zostały odnalezione w lokalnej bazie na urządzeniu.

**Administracja**

1. Urządzenie ma posiadać możliwość przywrócenia poprzednich zainstalowanych wersji firmware: ma być możliwość przywrócenia do wcześniej zainstalowanej wersji firmware lub do wersji, która została zainstalowana fabrycznie.
2. Urządzenie ma mieć możliwość przywrócenia poprzednio zainstalowanej bazy sygnatur wirusów.
3. Urządzenie ma mieć możliwość przywrócenia poprzednio zainstalowanej bazy sygnatur antyspamowych.
4. Urządzenie ma być konfigurowane za pomocą  graficznego interfejsu dostępnego przez przeglądarkę internetową.
5. Interfejs administratora ma być dostępny co najmniej w 16 różnych językach w tym w języku polskim.
6. Możliwość określenia czy administratorzy mają dostęp do interfejsu dostępnego przez przeglądarkę tylko poprzez protokół https.
7. Urządzenie ma mieć możliwość integracji z usługami katalogowymi LDAP oraz Active Directory przynajmniej do weryfikacji docelowych odbiorców przychodzących przesyłek pocztowych.
8. Urządzenie ma mieć możliwość skonfigurowania wirtualnych adresów IP do fizycznej karty sieciowej urządzenia.
9. Urządzenie ma mieć możliwość konfigurowania tras statycznych.
10. Urządzenie ma mieć możliwość przeprowadzenia diagnostyki poprzez interfejs graficzny przy użyciu narzędzi takich jak: ping, telnet, dig, tcpdump, traceroute.
11. Urządzenie ma mieć możliwość uruchomienia bezpiecznego, szyfrowanego połączenia z działem wsparcia technicznego producenta na życzenie administratora.
12. Urządzenie ma mieć możliwość tworzenia kopii zapasowej konfiguracji urządzenia,  ustawień wszystkich lub wybranych użytkowników.
13. Kopie zapasowe mają być tworzone na żądanie lub eksportowane zgodnie z harmonogramem na zdefiniowany serwer ftp i smb.
14. Możliwość określenia maksymalnej liczby plików kopii zapasowej przechowywanej na serwerze ftp i smb.
15. Możliwość tworzenia kopii zapasowej  baz danych filtrów Bayesa, dla całego systemu lub dla poszczególnych użytkowników.
16. Możliwość skonfigurowania adresu email, na który będą przesyłane kopie każdej wiadomości przychodzącej lub wychodzącej z urządzenia.
17. Oferowane rozwiązanie musi posiadać minimum pięcioletnią licencję obejmującą aktualizacje mechanizmów bezpieczeństwa m.in.:
18. Sygnatur antyspamu,
19. Sygnatur wirusów,
20. Bazy danych reputacji,
21. Analizy fingerprint,
22. Analizy intencji,
23. Reguł spamu obrazkowego,
24. Reguł spamu tradycyjnego.
25. Ochrona przed zero-day, tzw. sandboxing
26. Oferowane rozwiązanie musi zostać dostarczone z minimum pięcioletnią gwarancją sprzętową, obejmującą wymianę sprzętu w trybie Next Business Day i wsparcie producenta telefoniczne i mailowe 24/7 w j. angielskim. W przypadku bezawaryjnej pracy urządzenia przez min. 4 lata od zakupu, gwarancja sprzętowa musi obejmować bezpłatną wymianę urządzenia na nowe (z aktualnej na dzień wymiany oferty producenta). Wymiana urządzenia musi być realizowana przez producenta.

**Raportowanie**

System raportowania powinien być dostępny z poziomu przeglądarki:

1. Możliwość wyświetlenia natychmiastowych raportów
2. Możliwość zaplanowania raportów zgodnie z harmonogramem
3. Zestaw odstępnych raportów powinien obejmować co najmniej: nadawców spamu, odbiorców spamu, aktywność w rozsyłaniu wirusów, raport o nietypowych rozmiarach wiadomości, raport o naruszeniach protokołu SPF

**Usługi**

Wykonawca dostarczy rozwiązanie wraz z wdrożeniem systemu ochrony poczty do infrastruktury Zamawiającego i szkoleniem dla 4 uczestników, prowadzonym w j.polskim. Terminy wdrożenia i szkolenia zostaną uzgodnione z Wykonawcą.

……………………………………………………………………..

Miejscowość, data,

podpis osoby upoważnionej do reprezentowania Wykonawcy