Załącznik nr 1a
do SIWZ

Wymagania techniczne przedmiotu zamówienia

Część nr I

Dostawa licencji na oprogramowanie Anty-Spam 200 kont

Wymagania systemowe:
Dedykowane urządzenie z licencją lub licencja na środowisko wirtualne VMwareESXi/ESX/vSphere 4.x, 5.x lub Microsoft Hyper-V 2008/2012R2.
Integracja z LDAP: Active Directory (zarówno LDAP jaki Global Catalog), iPlanet Directory/Sun Directory Server 6.x/7.0, Lotus Domino LDAP Server 7.0/8.x, OpenLDAP 2.x

Funkcjonalność rozwiązania:
- Zintegrowane rozwiązanie antywirusowe, antyspamowe i filtrowania treści,
- Praca, jako bramka pocztowa,
- Blokowanie spamu w oparciu o lokalne polityki, silnik skanujący i bazy. Poczta nie jest przekierowana na serwer usługodawcy.
- Rozwiązanie antyspamowe ma mieć skuteczność nie mniejszą niż 98%. Równocześnie rozwiązanie ma charakteryzować się współczynnikiem fałszywych alarmów na poziomie 1 na milion, potwierdzonym przez niezależne testy.
- Do wykrywania spamu, system ma wykorzystywać bazy o numerach IP lub nazwach domen wykorzystywanych przez spamerów,
- System ma zapewnić routing wiadomości pocztowych w oparciu o domenę i adres odbiorcy,
- System ma mieć możliwość zmiany domeny i nazwy użytkownika w wiadomości przychodzącej i wychodzącej dla odbiorcy i nadawcy odpowiednio dla ruchu przychodzącego i wychodzącego,
- System ma umożliwiać tworzenie aliasów dla grup użytkowników,
- System ma zapewnić dopisywanie domyślnej nazwy domeny dla nadawcy wiadomości,
- System ma zapewnić ochronę przed skanowaniem serwera pocztowego w poszukiwaniu istniejących (prawidłowych) adresów pocztowych,
- Usuwanie nagłówków Received z wysyłanych wiadomości,
- Wiadomości z systemów próbujących atakować spamem serwer pocztowy, mają być automatycznie odrzucane przez określony czas, jeśli zostanie przekroczona wartość graniczna (ilość wiadomości zaklasyfikowanych, jako spam z jednego IP w danym przedziale czasu),
- Wiadomości z systemów próbujących atakować wirusami serwer pocztowy, mają być automatycznie odrzucane przez określony czas, jeśli zostanie przekroczona wartość graniczna (ilość wiadomości zaklasyfikowanych, jako wirusy z jednego IP w danym przedziale czasu),
- Połączenia z systemów próbujących atakować spamem serwer pocztowy, mają być automatycznie odrzucane przez określony czas, jeśli zostanie przekroczona wartość graniczna (ilość wiadomości zaklasyfikowanych, jako spam z jednego IP w danym przedziale czasu),
- Administrator ma mieć możliwość definiowania domen i adresów pocztowych, z którymi wymiana wiadomości będzie się zawsze odbywać,

- Administrator ma mieć możliwość definiowania domen i adresów pocztowych, z którymi wymiana wiadomości będzie zawsze blokowana,
- Niezależnie konfigurowane polityki dla wiadomości przychodzących i wychodzących,
- Funkcja ograniczająca dostępne pasmo dla maszyn/domen przesyłających spam, ale nieblokująca w całości komunikacji z tymi maszynami/domenami,
- Aktualizacje sygnatur spamu nie rzadziej, niż co 1 min,
- Aktualizacje sygnatur antywirusowych nie rzadziej, niż co 1 godzina,
- Rozwiązanie antywirusowy ma skanować skompresowane załączniki do 10 poziomów zagnieżdżeń w głąb i ma być odporna na złośliwie spreparowane załączniki („załączniki bomby"),
- Wiadomości z wirusami typu mass-mailer mają być w całości odrzucane, bez podejmowania dodatkowych akcji takich jak np. powiadomienie,
- Wykrywanie fałszywych URL-i w wiadomościach,
- Wykorzystanie technologii znakowania załączników dla odróżnienia ich treści,
- Wykorzystanie technologii analizy html mających na celu przeciwdziałanie metodom utrudniającym analizę treści wiadomości (np.: losowo generowane ciągi, nieprawidłowe kody formatujące),
- Detekcja języka, w którym została napisana wiadomość i możliwość użycia tej informacji, jako kryterium przy przetwarzaniu wiadomości,
- Kontrola treści w oparciu o słowa kluczowe lub słowniki definiowana przez administratora, w tym sprawdzanie zawartości skompresowanych archiwów,
- Zaawansowane mechanizmy tworzenia reguł kontroli treści, wiązanie wymagań przy pomocy logicznych I i LUB, możliwość budowanie reguł w postaci negatywnej NIE,
- Możliwość dodawania do wysyłanych wiadomości zdefiniowanego tekstu,
- Nakładanie polityk na załączniki w oparciu o ich rozmiar, typ MIME, nazwa pliku lub jego rozszerzenie – w tym identyfikację prawdziwego rozszerzenia pliku
- Wiadomości sklasyfikowane, jako spam można:
    - Usunąć
    - Dodać nagłówek wiadomości.
    - Zmodyfikować – dodać informację dla odbiorcy,
    - Zarchiwizować,
    - BCC – wysłać blind carboncopy na inny adres pocztowy,
    - Bounce – odpowiedzieć nadawcy wiadomością z modyfikowalnym NDR,
    - Wyczyścić, jeśli wiadomość zawierała wirusa,
    - Dostarczyć bez modyfikacji,
    - Przekierować na inny adres pocztowy,
    - Zmodyfikować temat wiadomości,
    - Wrzucić wiadomość do centralnej kwarantanny,
    - Przesłać powiadomienie na wybrany adres,
    - Usunąć załącznik z wiadomości,
- Możliwość wysłania wiadomości spam niewykrytych przez rozwiązanie do producenta, w celu ich analizy,
- Rozróżnienie kategorii wiadomości na:
    - Normalne wiadomości bez spamu i wirusów,
    - Spam,
    - Podejrzane o spam,
    - Biuletyn (tzw. newsletter),
    - Wiadomość marketingowa
    - Wiadomość z podejrzanym adresem URL,

    - Wirusy masowe,
    - Wiadomości zawierające wirusy,
    - Wiadomości, których nie można przeskanować,
    - Wiadomości od blokowanych nadawców,
    - Wiadomości zablokowane na podstawie filtrów przygotowanych przez administratora,
- Wsparcie dla Transport Layer Security (TLS) – definiowane per domena lub polityka, Sender Policy Framework (SPF), Sender ID
- Import bazy użytkowników poprzez LDAP,
- Administrator ma mieć możliwość ingerencji w czułości rozwiązania,
- Rozwiązanie ma posiadać serwer kwarantanny. Serwer ma być dostępny dla poszczególnych użytkowników końcowych. Serwer ma przesyłać okresowe powiadomienia o zawartości kwarantanny. Powiadomienia mają mieć wbudowane mechanizmy do zarządzania zawartością kwarantanny (przesłanie dalej, podgląd, zalogowanie do kwarantanny),
- Na serwer kwarantanny można nałożyć ograniczenia dla poszczególnych użytkowników jak i całego serwera wg ilości przechowywanych wiadomości, ilości zajętego miejsca,
- Użytkownik końcowy rozwiązania ma mieć możliwość definiowania własnych list blokowanych i przepuszczanych nadawców wiadomości, ingerencje w zachowanie systemu detekcji języka i możliwość wysłania do producenta systemu źle sklasyfikowanych wiadomości,
- Komunikacja pobierania uaktualnień ma być szyfrowana.
- Komunikacja w celu zarządzania systemem ma być szyfrowana.
- Rozwiązanie ma być centralnie zarządzane z wbudowanymi mechanizmami raportowania. Jedna konsola ma umożliwić zarządzania kilkoma współpracującymi urządzeniami. Wykonywane raporty mają uwzględniać dane zebrane ze wszystkich współpracujących urządzeń.
- System ma posiadać przynajmniej 55 wbudowanych raportów. Wykonanie raportów można zaplanować w dzienniku. Gotowe raporty można przesłać do skrzynki pocztowej wyznaczonych odbiorców.
- System ma umożliwiać tworzenie wielu kont administracyjnych z różnymi poziomami uprawnień, w tym możliwość zdefiniowania użytkowników mających dostęp do różnych kwarantann,
- System ma umożliwiać definiowanie poziomu logowania o swojej aktywności.
- System ma powiadamiać wybranych administratorów o nieprawidłowej pracy komponentów,
- System ma umożliwiać wykonywanie zaplanowanych kopii bezpieczeństwa konfiguracji i baz kwarantanny oraz możliwość odtworzenia konfiguracji z tak wykonanej kopii.
- Ograniczony zestaw poleceń dostępny z konsoli systemu operacyjnego,
- System ma umożliwiać graficzne śledzenie wiadomości, w tym informacje, co stało się z wiadomością,
- System ma posiadać wewnętrzną bazę reputacji, śledzącą adresy IP serwerów pocztowych
- System ma umożliwiać zapytanie o adres IP do wewnętrznej i globalnej bazy reputacji
- System ma umożliwiać stworzenie odpowiednio obsługiwanych kolejek z punktu widzenie reputacji danego adresu IP – ograniczając taki adres do ilości wysyłanych wiadomości, ilości nawiązywanych połączeń w określonym czasie
- System ma mieć możliwość zdefiniowania osobnej kwarantanny dla poczty naruszającej reguły zgodności z polityką określającą rodzaj przesyłanych treści
- System musi umożliwiać skorzystania z predefiniowanych polityk i wzorców

- System ma umożliwiać rozpatrywanie incydentów skojarzonych z naruszeniem polityk, w tym definiowanie ważności incydentu.
- Rozpatrując incydent muszą być z góry określone akcje, które osoba rozpatrująca incydent może podjąć, np. rozpoczęcie śledztwa, przesłanie widomości do odbiorcy, przesłanie wiadomości do nadawcy, itp.
- System ma posiadać ochronę przed atakami wirusów typu Day Zero, oraz zdefiniowaną kwarantannę dla złapanych w ten sposób wirusów z możliwością ustawienia czasu, przez który zatrzymane maile mają w niej pozostawać
- System musi umożliwiać wysyłkę źle sklasyfikowanych wiadomości typu spam do producenta, gdzie automatycznie zostaną przygotowane sygnatury antyspamowe i natychmiast dostarczone do rozwiązania
- System ma dodatkowo posiadać możliwość wysyłania alertów SNMP
- System ma umożliwiać integrację z UPS-em
- System musi wspierać autentykację DomainKeysIdentified Mail (DKIM)
- System musi wspierać autentykację SMTP
- System musi wykorzystywać Bounce Attack Tag Validation (BATV)
- System musi zapewniać dedykowaną ochronę dla potencjalnie niebezpiecznej zawartości (makra, skrypty, osadzony Flash, itp.) znajdującej się w plikach PDF oraz plikach pakietu Microsoft Office, polegającą na przebudowaniu takiego dokumentu, usuwając z niego potencjalnie niebezpieczną zawartość według określonego kryterium – usuwaj Flash, pozostaw makra.
- Licencja na 200 kont użytkowników