NZM.231.7.2017.DM **Załącznik nr 3 do OPZ**

Dostawa kompletnego rozwiązania obsługi poczty

Zadanie III

Kompletne rozwiązanie obsługi poczty	
Parametr	**Opis**
Architektura systemu ochrony	System ochrony musi zapewniać kompleksową ochronę antyspamową, antywirusową i antyspyware'ową. Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny pochodziły od jednego producenta, który udzieli odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie). System powinien być dostarczony w postaci komercyjnej platformy działającej w środowisku wirtualnym z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESXi / ESX 4.0 / 4.1 / 5.0 / 5.1/5.5/6.0
System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia.
Parametry systemu	Obsługa nie mniej niż 4 interfejsów Ethernet 10/100/1000 Base-TX Powierzchnia dyskowa - minimum 1 TB (z możliwością rozbudowy do 2 TB)
Sposoby implementacji	Urządzenie powinno mieć możliwość pracy w każdym z trzech trybów: • Tryb gateway • Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej) • Tryb serwera pocztowego

Funkcjonalności	System musi realizować poniższe funkcjonalności w każdym z trzech trybów pracy: • Wsparcie dla wielu domen pocztowych • Polityki filtrowania tworzone w oparciu o adresy mailowe, nazwy domenowe, adresy IP (w szczególności reguła all-all) • Email routing oraz zarządzanie kolejkami bazujące na politykach • Ochrona poczty przychodzącej oraz wychodzącej • Granularne, wielowarstwowe polityki wykrywania spamu oraz wirusów • Skanowanie Antywirusowe oraz Antyspamowe definiowane na użytkownika w oparciu o atrybuty LDAP • Routing poczty (email routing) w oparciu o LDAP • Kwarantanna poczty z dziennym podsumowaniem (możliwość samodzielnego zwalniania plików z kwarantanny przez użytkownika) • Dostęp do kwarantanny poprzez WebMail lub POP3 • Archiwizacja poczty przychodzącej i wychodzącej, backup poczty do różnych miejsc przeznaczenia • Uwierzytelnianie SMTP w oparciu o protokoły: LDAP, RADIUS, POP3, IMAP • Mechanizmy reputacji nadawcy wiadomosci • Whitelist'y definiowane dla użytkownika
Funkcjonalności w trybie serwera pocztowego	System musi zapewniać: • Obsługę serwisów pocztowych: SMTP, POP3, IMAP • Wsparcie SMTP over SSL • Definiowanie powierzchni dyskowej dla użytkowników • Szyfrowany dostęp do poczty poprzez WebMail • Polski interfejs użytkownika przy dostępie przez WebMail • Kalendarz na WebMail'u • Lokalne konta użytkowników oraz uwierzytelnianie w oparciu o LDAP • Synchronizacja książki adresowej z LDAP
Ochrona antywirusowa, antyspyware'owa	System musi realizować: • Skanowanie antywirusowe wiadomości SMTP • Kwarantannę dla zainfekowanych plików • Skanowanie załączników skompresowanych • Definiowanie komunikatów powiadomień w języku polskim • Blokowanie załączników ze względu na typ pliku

Ochrona antyspamowa	System musi zapewniać niżej wymienione metody filtrowania spamu: • Heurystyczna analiza poczty z dynamiczną aktualizacją reguł • Filtrowanie treści załączników, filtrowanie wiadomości po słowach kluczowych • Szczegółowa kontrola nagłówka wiadomości • Filtrowanie w oparciu o filtry Bayes'a, z możliwością dostrajania dla poszczególnych użytkowników • Filtrowanie poczty w oparciu o sumy kontrolne spamu • Wykrywanie spamu w oparciu a analizę plików graficznych oraz plików PDF • Analiza poczty w oparciu o dynamiczną bazę spamu dostarczaną przez tego samego producenta • Współpraca z zewnętrznymi serwerami RBL • Kontrola w oparciu o Greylist'y • Białe i czarne listy definiowane globalnie oraz per użytkownik • Weryfikacja źródłowego adresu IP • Mechanizmy reputacji użytkownika • Możliwe akcje dla poczty: Accept, Relay, Reject,, Discard, Kwarnatanna, Oznaczanie (Tagging)
Ochrona przed atakami DoS	• Denial of Service (Mail Bombing) • Ochrona przed atakami na adres odbiorcy • Definiowanie maksymalnych ilości wiadomości pocztowych • Kontrola Reverse DNS (Anty-Spoofing) • Weryfikacja poprawności adresu e-mail nadawcy
Parametry wydajnościowe i niezawodnościowe	• ochrona minimum 80 domen pocztowych • obsługa min 400 lokalnych skrzynek pocztowych w trybie serwer • Obsługę nie mniej niż 50 profili antywirusowych lub antyspamowych • Skanowanie Antyspamowe min. 50 tyś wiadomości/godzinę
Bezpieczeństwo wiadomości	• System powinien zapewniać mechanizmy szyfrowania wysyłanych wiadomości pocztowych, bez konieczności instalowania jakichkolwiek aplikacji na stacjach klienckich. Administrator powinien mieć możliwość włączenia tej funkcjonalności dla wybranych użytkowników. • Wsparcie dla szyfrowanej komunikacji Gateway-to-Gateway • Wsparcie dla szyfrowanych protokołów: HTTPS, SMTPS, IMAPS, POP3S
Logowanie i raportowanie	• Możliwość definiowania polityki w oparciu w wbudowany kreator konfiguracji • Logowanie SNMP dla zdarzeń systemowych oz możliwością definiowania progów • Logowanie do zewnętrznego serwera SYSLOG • Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych • Powiadamianie o działalności wirusów • Logowanie informacji na temat spamu oraz niedozwolonych załączników • Predefiniowane szablony raportów • Możliwość planowania czasu generowania raportów • Możliwość podglądu logów w czasie rzeczywistym • Archiwizacja poczty w oparciu o zestaw filtrów (np. słowa kluczowe)

Tryb wysokiej dostępności (HA)	System musi zapewniać: • Konfigurację HA [Active-Passive] w każdym z trybów: gateway, transparent, serwer • Tryb Active-Passive z syncronizacją polityk i wiadomości, gdzie cluster występuje pod jednym adresem IP • Tryb synchronizacji konfiguracji dla scenariuszy rozległych (osobne adresy IP) • Wykrywanie awarii i powiadamianie administratora • Monitorowanie stanu połączeń
Aktualizacje sygantur, dostęp do bazy spamu	System musi zapewniać: • Pracę w oparciu o bazę spamu uaktualnianą w czasie rzeczywistym • Planowanie aktualizacji szczepionek antywirusowych w czasie (Scheduler) • Wymuszona aktualizacja bazy wirusów (tryb push)
Zarządzanie i Raportowanie	• Lokalny interfejs zarządzania poprzez szyfrowane połączenie HTTPS, SSH • Definiowanie wyglądu interfejsu zarządzania z możliwością wstawienia logo firmy
	• Instalacja i konfiguracja systemu powinna być przeprowadzona przez uprawnionego inżyniera • Wykonawca powinien zapewnić pierwszą linie wsparcia technicznego telefonicznie w języku polskim w trybie 8x5

Gwarancja	1) Gwarancja: *System powinien być objęty serwisem gwarancyjnym producenta przez okres 36miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, Wykonawca winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej.* *2)* Gwarancja: *System powinien być objęty serwisem gwarantującym udostępnienie i dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym /w ciągu 8 godzin/. Serwis powinien być realizowany przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta w zakresie serwisu gwarancyjnego (Wykonawca winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Polski), mających swoją siedzibę na terenie Polski. Zgłoszenia serwisowe przyjmowane w trybie 8x5 / 24x7 przez dedykowany serwisowy moduł internetowy (należy podać adres www) oraz infolinię 24x7 (należy podać numer infolinii).* 3) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): *W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw.* produkty podwójnego zastosowania)*, Wykonawca 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. 4) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): *Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.*

Wykonawca w ofertowej „Specyfikacji technicznej" bezwzględnie musi określić nazwę, producenta i model oferowanego urządzenia komputerowego, jak i pozostałe wymogi (gwarancja, certyfikaty, autoryzacje, itp.) Jeżeli zaś chodzi o elementy sprzętu - wystarczającym będzie dokładne określenie oferowanych parametrów technicznych (np. obsługiwane protokoły, typy szyfrowania, itp.), tak aby

Zamawiający mógł porównać i stwierdzić, że oferowany sprzęt spełnia określone wymagania, (nie może być sformułowań nieprecyzyjnych takich jak „lub”, „np.”, „nie mniejsze niż”, „zbliżone”, itp.); z oferty powinno jasno wynikać, jaki rodzaj sprzętu i podzespoły oferuje Wykonawca.