*Załącznik nr 1b do umowy projekt* *dla zadania nr 2*

**FORMULARZ RZECZOWY**

**OPIS OFEROWANEGO PRZEDMIOTU ZAMÓWIENIA**

**Zadanie 2**

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P.** | **Urządzenie** | **Wymagane minimalne \*** | **Oferowane parametry****WYPEŁNIA WYKONAWCA** |
| 1 | Urządzenie do kompleksowej ochrony poczty elektronicznej | 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 ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systemu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure.Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń. Dostarczone rozwiązanie musi mieć możliwość pracy w każdym z trybów:1.Tryb Gateway.2.Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej). |  |
| Parametry fizyczne systemu antyspamowego | System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności, co najmniej 1 TB. |  |
| Serwer 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, TLS 1.2 oraz TLS 1.3).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. 25 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.Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.7.Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.8.Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.9.Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.10.Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.11.Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.12.Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.13.Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.14.Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.15.Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.16.Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.17.Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika. |  |
| 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.Definiowanie 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 4 lokalnych kont administracyjnych. |  |
| Asysta techniczna on-line | 1.Asysta techniczna przy wdrożeniu będzie wykonana przez inżyniera z certyfikatem producenta.2.Zakres działań podczas wdrożenia:•Przygotowanie środowiska (rejestracja i instalacja maszyny wirtualnej, aktualizacja oprogramowania).•Konfiguracja ustawień antywirusowych, przygotowanie polityk, ustawienie IP reputation•Weryfikacja poprawności implementacji (testy akceptacyjne).•Kopia bezpieczeństwa konfiguracji wdrożonych urządzeń.•Instruktarz obsługi urządzenia poprzez GUI (co najmniej 2 godziny) przeprowadzony przez inżyniera. |  |
| Certyfikaty | Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji: VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified. |  |
| Serwisy i licencje | System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake na okres wskazany w ofercie. | **na okres …. miesięcy** ***(wpisać to samo co  w pkt 4 oferty*** *i)* |
| Gwarancja oraz wsparcie | System musi być objęty serwisem producenta przez okres wskazany w ofercie, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. |
| Oferowany model Urządzenia ***(wymienić również wszystkie oferowane z urządzeniem licencje i serwisy***) |  |

\* W Załączniku zawarto minimalne wymagania odnośnie produktów objętych zamówieniem co oznacza, że Wykonawca może zaoferować przedmiot zamówienia charakteryzujący się lepszymi parametrami technicznymi lub użytkowymi.

UWAGA: Niespełnienie wymagań minimalnych określonych w powyższym formularzu skutkować będzie odrzuceniem oferty

Wykonawca wypełnia tylko pola w kolorze białym, ze szczególnym uwzględnieniem pól dotyczących serwisów, licencji, gwarancji oraz wsparcia, gzie koniecznie musi podać tylko jeden okres ( np. 12 miesięcy). Inne zapisy będą interpretowane jako niespełnienie wymagań oraz spowodują odrzucenie oferty.

………………………………………………………………….

**.**

 **Data,** ELEKTRONICZNY PODPIS WYKONAWCY lub

osoby uprawnionej do składania oświadczeń woli

 w imieniu Wykonawcy, w postaci:

- kwalifikowanego podpisu elektronicznego,

- **LUB** podpisu zaufanego, - **LUB** podpisu osobistego e-dowód.