Załącznik Nr 3
do Ogłoszenia o zamówieniu

Wzór umowy

UMOWA NR [_]

zawarta w dniu [_] 2021 roku, w Poznaniu pomiędzy:

Specjalistycznym Zespołem Opieki Zdrowotnej nad Matką i Dzieckiem w Poznaniu, Samodzielny Publiczny Zakład Opieki Zdrowotnej ul. Krysiewicza 7/8, 61-825 Poznań wpisanym do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej prowadzonego przez Sąd Rejonowy Poznań - Nowe Miasto i Wilda w Poznaniu, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS: 0000003220, posługującym się nadanym jej Numerem Identyfikacji Podatkowej: 778-11-28-565 oraz REGON: 630863147.
zwanym dalej ***„Zamawiającym"***,

reprezentowanym przez:

[_] - [_]

a

(w przypadku przedsiębiorcy wpisanego do KRS)
Spółką działającą pod firmą [_], z siedzibą w [_] przy ulicy [_], kod pocztowy [_], wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS: [_], której akta rejestrowe są przechowywane w [_], posługującej się nadanym jej Numerem Identyfikacji Podatkowej [_] oraz numerem REGON [_]
zwaną w dalszej treści umowy **„Wykonawcą"**

reprezentowaną przez:

[_] - [_]

(w przypadku przedsiębiorcy wpisanego do CEIDG)
(imię i nazwisko) [_], prowadzącym działalność gospodarczą pod nazwą [_] z siedzibą przy ulicy [_], kod pocztowy [_], wpisaną do Centralnej Ewidencji i Informacji o Działalności Gospodarczej Rzeczypospolitej Polskiej pod numerem PESEL [_], Numerem Identyfikacji Podatkowej [_] oraz numerem REGON [_]

zwanym w dalszej treści umowy **„Wykonawcą"**.

Strony zgodnie oświadczają, że osoby je reprezentujące przy zawieraniu niniejszej umowy (zwanej dalej: *„Umową"*) są do tego prawnie umocowane zgodnie z wymogami prawa polskiego. W związku z powyższym nie będą powoływać się na brak umocowania osoby reprezentującej w przypadku jakichkolwiek sporów mogących wyniknąć z Umowy.

Niniejsza Umowa zostaje zawarta w wyniku przeprowadzonego postępowania o udzielenie zamówienia publicznego zgodnie z Regulaminem udzielania zamówień publicznych na podstawie art. 2 ust 1 pkt 1 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 2019 z późn. zm.) dla zamówienia o wartości szacunkowej nieprzekraczającej kwoty 130 000,00 złotych netto (bez podatku od towarów i usług).

Zamawiający i Wykonawca, zwani w dalszej części z osobna również *„Stroną"*, zaś wspólnie *„Stronami"*, zawierają niniejszą Umowę, o następującej treści:

§ 1.
Przedmiot Umowy

1. Przedmiotem Umowy jest: **Dostawa systemu poczty elektronicznej wraz z wdrożeniem.**
2. Szczegółowy opis Przedmiotu Umowy określony ostał w załączniku Nr 1 do Umowy – Szczegółowe warunki zamówienia.

§ 2.
Warunki dostawy

1. Termin wykonania wynosi: 30 od daty zawarcia umowy.
2. Termin, o którym mowa w ust. 1 uważa się za zachowany w momencie dostarczenia aktywnych kluczy licencyjnych na adres poczty elektronicznej Zamawiającego: jan.lis@szoz.pl i potwierdzenia ich otrzymania na adres poczty elektronicznej Wykonawcy ..... .
3. Za dzień roboczy uznaje się dzień tygodnia od poniedziałku do piątku, w godzinach od 8:00 do 15:00, z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych u Zamawiającego.
4. Wykonawca zobowiązuje się do objęcia serwisem producenta dostarczonego serwisu przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
5. W przypadku stwierdzenia nieprawidłowości w dostarczonych przez Wykonawcę kluczach licencyjnych, Zamawiający odmówi podpisania Protokołu odbioru i wyznaczy Wykonawcy dodatkowy termin nie dłuższy jednak niż 5 dni roboczych na dostarczenie przedmiotu Umowy wolnego od wad.
6. Do współpracy i koordynacji realizacji Przedmiotu Umowy, w tym do podpisywania Protokołu Odbioru upoważnione są osoby ze strony Zamawiającego:
   1) .....tel.: .....e-mail:.....
   lub
   2) .....tel.: .....e-mail:.....
7. Do współpracy i koordynacji realizacji Przedmiotu Umowy, w tym do podpisywania Protokołu Odbioru upoważnione są osoby ze strony Wykonawcy:
   1) .....tel.: .....e-mail:.....
8. Wykonawca zapewnia Zamawiającemu wsparcie techniczne, przez okres określony w ust. 4. W przypadku gdy nie będzie ono działać poprawnie (wady fizyczne), pomimo ich prawidłowej instalacji, Wykonawca zobowiązuje się wymienić niezwłocznie wadliwy system na nowe lub usunąć wady.
9. Za wady fizyczne systemu Strony przyjmują:
   1) nieistnienie w systemie wszystkich deklarowanych modułów;
   2) niewykonywanie lub nienależyte wykonywanie przez system wszystkich lub niektórych określonych przez producenta funkcji;
   3) brak zasadniczej bezbłędności wykonywania przez system jego podstawowych funkcji;
   4) niezdolność oprogramowania do pracy w określonym przez producenta systemie operacyjnym i przy określonych wymaganiach sprzętowych.
10. Wszelkie koszty związane z wymianą systemu będącego Przedmiotem Umowy na wolne od wad ponosi Wykonawca.

§ 3.
Wynagrodzenie

1. Wynagrodzenie Wykonawcy z tytułu prawidłowego wykonania przedmiotu Umowy wynosi:
   Wartość brutto: ..... zł
   (słownie: ..... zł).
2. Zapłata wynagrodzenia nastąpi na podstawie prawidłowo wystawionej przez Wykonawcę faktury/rachunku, przelewem na rachunek bankowy Wykonawcy podany na fakturze/rachunku, w terminie do 60 dni od dnia jej doręczenia do siedziby Zamawiającego.
3. Podstawą do wystawienia faktury/rachunku jest podpisany przez Strony Protokół odbioru wnioskujący o rozliczenie finansowe.
4. Płatność będzie dokonywana przelewem na rachunek bankowy Wykonawcy: .....
5. Za dzień zapłaty uważany będzie dzień obciążenia rachunku Zamawiającego.

§ 4.
Licencja.

1. W związku z zawarciem Umowy Zamawiający, z zastrzeżeniem ust. 2, nabywa prawo do legalnego korzystania z systemu na warunkach wskazanych przez producenta tego systemu oraz na warunkach wskazanych w Umowie.
2. Przed podpisaniem Protokołu odbioru, Wykonawca dostarczy Zamawiającemu licencję *(dokument zapewniający Zamawiającemu prawo do korzystania z systemu)* na następujących polach eksploatacji:
   1) korzystania z systemu w ramach wszystkich funkcjonalności w dowolny sposób w zakupionej liczbie,
   2) odtwarzania;
   3) pobierania;

4) uruchamiania;
5) przechowywania;
6) wyświetlania;
7) instalowania i deinstalowania systemu pod warunkiem zachowania liczby udzielonych licencji;
8) sporządzania kopii zapasowej *(kopii bezpieczeństwa)* nośników instalacyjnych i nośników z zainstalowanym systemów;
9) korzystania z produktów powstałych w wyniku eksploatacji systemu przez Zamawiającego, w szczególności danych, raportów, zestawień oraz innych dokumentów kreowanych w ramach tej eksploatacji oraz modyfikowania tych produktów i dalszego z nich korzystania.

3. Wykonawca oświadcza, że dostarczony przez niego system nie narusza jakichkolwiek praw osób trzecich, zwłaszcza w zakresie przepisów o wynalazczości, znakach towarowych, prawach autorskich i prawach pokrewnych oraz nieuczciwej konkurencji, i że posiada prawo do odsprzedaży/udzielania licencji/sublicencji na system, na które Wykonawca udzielił licencji Zamawiającemu, zgodnie z postanowieniami Umowy i przejmuje w tym zakresie odpowiedzialność w przypadku roszczeń osób trzecich.
4. Wykonawca uprawnia Zamawiającego do swobodnego dokonywania zmian w zakresie przydzielania poszczególnych licencji pracownikom Zamawiającego, do systemu, na które Wykonawca udzielił licencji.
5. Zamawiający zobowiązuje się:
   1) korzystać z systemu wyłącznie dla własnych potrzeb;
   2) nie udostępniać systemu odpłatnie ani nieodpłatnie do użytkowania osobom trzecim;
   3) nie usuwać znaków handlowych oraz znaków autorskich z systemem i z dokumentacji;
   4) nie dokonywać zmian w systemie, a w szczególności nie dokonywać adaptacji na inny język programowania, jak również nie umożliwiać takich czynności osobom trzecim.

§ 5.

Odstąpienie od Umowy. Kary umowne

1. Zamawiającemu przysługuje prawo odstąpienia od Umowy w przypadku gdy Wykonawca:
   a) przedstawił nieprawidłowe lub niezgodne ze stanem faktycznym informacje będące podstawą do wypłaty wynagrodzenia,
   b) bez uzasadnienia nie wykonuje lub nienależycie wykonuje przedmiotu Umowy i pomimo wezwania go do zmiany sposobu ich wykonywania nadal wykonuje je nienależycie lub wcale nie wykonuje,
   c) powierzył wykonanie przedmiotu Umowy osobie trzeciej bez zgody Zamawiającego,
   d) naruszył przy wykonywaniu Umowy prawa osób trzecich.
   – w terminie 30 dni od zaistnienia ww. zdarzeń.
2. Zamawiający zastrzega sobie prawo do odstąpienia od Umowy w razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie zamówienia nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy, lub dalsze wykonywanie Umowy może zagrozić istotnie interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu Zamawiający może odstąpić od Umowy w terminie do 30 dni od powzięcia wiadomości o powyższych okolicznościach.
3. Zamawiającemu przysługuje prawo odstąpienia od Umowy, jeżeli dostarczone klucze licencyjne nie spełniają swojej funkcji. Prawo odstąpienia należy wykonać w terminie 30 dni od powzięcia wiadomości o tej okoliczności.
4. W przypadku niedotrzymania któregokolwiek terminu, o którym mowa w § 2 ust.1 lub § 2 ust. 5, Zamawiający zastrzega sobie prawo obciążenia Wykonawcy karami umownymi w wysokości 1% wynagrodzenia, o którym mowa w § 3 ust. 1, za każdy dzień zwłoki.
5. W przypadku odstąpienia od Umowy z przyczyn, za które odpowiedzialność ponosi Wykonawca, Zamawiający zastrzega sobie prawo obciążenia Wykonawcy karą umowną w wysokości 15% wynagrodzenia, o którym mowa w § 3 ust. 1.
6. Zamawiający zastrzega sobie możliwość dochodzenia na zasadach ogólnych odszkodowania przewyższającego ustalone kary umowne.

§ 6.

Postanowienia końcowe

1. Przez „siłę wyższą" Strony rozumieją zdarzenie nagłe, nieprzewidziane i niezależne od woli Stron, którego skutki są niemożliwe do zapobieżenia, uniemożliwiające wykonanie umowy w całości lub części, na stałe lub na pewien czas, któremu nie można zapobiec ani przeciwdziałać przy zachowaniu należytej staranności. W szczególności za siłę wyższą uznaje się pożar, powódź, epidemię, trzęsienia ziemi, awarię zasilania lub naturalnych źródeł energii, huragany i inne katastrofy naturalne, a także stany nadzwyczajne i wyjątkowe, w tym stan wojny,

stan wojenny, stan klęski żywiołowej, stan epidemii, stan zagrożenia epidemicznego, a także strajki, bojkoty, zamachy terrorystyczne, blokady komunikacyjne o charakterze ponadregionalnym, a także przypadki wydawania przez władze krajowe i lokalne aktów prawnych wprowadzających ograniczenia, nakazy lub zakazy określonego zachowania się, niezależnie od formy takiego aktu oraz tego czy zagrażają w chwili obecnej.

2. W razie wystąpienia przypadku ,,siły wyższej" mającego negatywny wpływ na prawidłowe realizowanie postanowień Umowy, strona dotknięta ,,siłą wyższą", zostaje zwolniona ze swoich zobowiązań wynikających z Umowy, na czas występowania ,,siły wyższej" a uzgodnione terminy zostaną odpowiednio przedłużone.
3. W razie wystąpienia przypadku ,,siły wyższej" strona, która ze względu na ,,siłę wyższą" nie może zrealizować swoich zobowiązań jest zobowiązana powiadomić pisemnie o tym fakcie drugą stronę oraz podać dane na temat okoliczności ,,siły wyższej" oraz ich wpływu na realizację zobowiązań.
4. Po ustaniu „siły wyższej" strona dotknięta działaniem „siły wyższej", jest zobowiązana niezwłocznie powiadomić pisemnie drugą stronę o fakcie ustania okoliczności lub zdarzeń „siły wyższej". Po otrzymaniu zawiadomienia strony ustalają nowy termin realizacji.

§ 7

1. Strony zgodnie postanawiają, że wynikające z Umowy prawa lub obowiązki Wykonawcy nie mogą być przeniesione na osobę trzecią bez uprzedniej zgody Zamawiającego, wyrażonej na piśmie pod rygorem nieważności (art. 509 Kodeksu Cywilnego).
2. Strony zgodnie postanawiają, że wynikające z Umowy wierzytelności Wykonawcy nie mogą być przedstawiane do potrącenia (art. 498 Kodeksu Cywilnego) z wierzytelnościami Zamawiającego.
3. Wszelkie zmiany Umowy mogą być dokonywane wyłącznie na piśmie pod rygorem nieważności.
4. Należności wynikające z Umowy łącznie z odszkodowawczymi i odsetkowymi nie mogą być przedmiotem obrotu (cesja, sprzedaż), zgodnie z art. 509 KC, bez pisemnej zgody Zamawiającego.
5. Wszelkie powiadomienia, zgody, akceptacje, zatwierdzenia itp., składane przez Zamawiającego w związku z Umową, mogą być przesłane Wykonawcy również drogą elektroniczną na adres e-mail Wykonawcy podany w Umowie lub na inny wskazany pisemnie Zamawiającemu przez Wykonawcę adres e-mail, ze skutkiem doręczenia bez obowiązku składania podpisu elektronicznego.
6. Wszelkie spory wynikłe z realizacji Umowy rozstrzyga właściwy miejscowo i rzeczowo dla siedziby Zamawiającego Sąd Powszechny.
7. W sprawach nieuregulowanych Umową mają zastosowanie przepisy kodeksu cywilnego.
8. W trakcie realizacji Umowy, w przypadku konieczności dostępu Wykonawcy do danych osobowych ze zbiorów prowadzonych przez Zamawiającego, stosownie do art. 28 ust. 3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 2016 r., str. 1-88), Strony postanawiają zawrzeć, przed uzyskaniem przez Wykonawcę dostępu do danych osobowych ze zbiorów, o których mowa powyżej, Umowę powierzenia przetwarzania danych osobowych według wzoru określonego przez Zamawiającego. W przypadku opóźnienia przez Wykonawcę podpisania Umowy powierzenia przetwarzania danych osobowych, Zamawiający wstrzyma się z udostępnieniem Wykonawcy wszelkich danych osobowych. W takim przypadku wszelkie ryzyka związane ze wstrzymaniem się przez Zamawiającego od udostępnienia Wykonawcy jakichkolwiek danych osobowych obciążają Wykonawcę.

§ 8

Umowa spisana została w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

<u>Załączniki do Umowy:</u>

1. Załącznik nr 1 „Szczegółowe warunki zamówienia".

ZAMAWIAJĄCY **WYKONAWCA**

Załącznik nr 1 do Umowy

Szczegółowe warunki zamówienia.

1. Oferowane produkty muszą spełniać wszystkie parametry określone poniżej oraz pochodzić z legalnego źródła, muszą być dostarczone przez autoryzowany kanał sprzedaży producenta na terenie kraju i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i oprogramowania świadczonych przez sieć serwisową producenta na terenie Polski. Zamawiający zastrzega sobie prawo do żądania potwierdzenia źródła pochodzenia urządzenia w postaci oświadczenia producenta.
2. Wykonawca musi dostarczyć sprzęt z niezbędnym okablowaniem.
3. Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

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, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o dedykowany system operacyjny oraz 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).

Parametry fizyczne systemu antyspamowego

System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 2 TB.

Funkcja serwera poczty

W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 400 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 100 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 50 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 POP3.
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 Preention).

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 400 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.

Kontrola antyspamowa

System musi zapewniać poniższo 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 poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu a 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 400 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.
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.
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 6 lokalnych kont administracyjnych.

Certyfikaty

Dostarczony system powinien posiadać poniższe certyfikaty:

1. VBSpam and VB100 rated lub 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: kontrole Antyspam, URL Filtering, kontrola antywirusowa na okres 12 miesięcy.

Gwarancja oraz wsparcie

System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Opisy do wymagań ogólnych

Opis przedmiotu zamówienia (nie techniczny, tylko ogólny):

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. Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Zamawiający wymaga wykonanie konfiguracji systemu antyspam:

- Instalacja maszyny wirtualnej w środowisku Zamawiającego.
- Konfiguracja sieciowa urządzenia.
- Konfiguracja przestrzeni dyskowej na skrzynki mailowe za pomocą NFS lub iSCSI.
- Konfiguracja chronionej domeny mailowej.
- Konfiguracja profili dostępowych dla administratorów.
- Integracja systemu z Active Directory za pomocą protokołu LDAP.
- Konfiguracja profili zabezpieczających przed złośliwym oprogramowaniem, spamem oraz niedozwolonymi treściami
- Konfiguracja kwarantanny.
- Konfiguracja reguł pocztowych z użyciem zdefiniowanych profili zabezpieczających.
- Konfiguracja logowania zdarzeń i raportowania.
- Migracja zawartości obecnych skrzynek pocztowych do nowego systemu.
- Testy i monitorowanie po przełączeniu produkcyjnym.