Załącznik nr 3 do SWZ

Numer referencyjny postępowania:
SZP/DIT/31/2023

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA NA ZADANIE: „DOSTAWA SYSTEMU DO KOMPLEKSOWEJ OCHRONY POCZTY ELEKTRONICZNEJ"

Przedmiotem zamówienia jest „**Dostawa systemu do kompleksowej ochrony poczty elektronicznej"**

I. WYMAGANIA OGÓLNE

1. System ochrony poczty powinien zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników.
2. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
3. Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie powinno pracować w oparciu o komercyjne bazy zabezpieczeń.
4. Dostarczone rozwiązanie powinno mieć możliwość pracy w każdym trybów:

a. Tryb Gateway.
b. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

II. PARAMETRY FIZYCZNE SYSTEMU ANTYSPAMOWEGO

1. System powinien być wyposażony w interfejsy: 4 porty Gigabit Ethernet RJ-45.
2. System powinien być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 2 TB z możliwością obsługi mechanizmu RAID 0,1
3. System powinien posiadać wbudowany port konsoli szeregowej.
4. Zasilanie z sieci 230V/50Hz.

III. OGÓLNE FUNKCJE SYSTEMU OCHRONY POCZTY

1. Dostarczany system obsługi i ochrony poczty powinien zapewniać poniższe funkcje:

a) Wsparcie dla co najmniej 100 domen pocztowych.
b) System powinien realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 150 tys. wiadomości/godzinę.
c) Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
d) Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
e) Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
f) 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.

tel. (61) 8310-142; 8310-242
email: zamowienia.publiczne@orsk.pl

g) Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
h) Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
i) Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
j) Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
k) Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
l) Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
m) Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
n) Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
o) Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
p) Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
q) Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.

2. Kontrola antywirusowa i ochrona przed malware

W tym zakresie dostarczony system ochrony poczty powinien zapewniać:

a) Skanowanie antywirusowe wiadomości SMTP.
b) Kwarantannę dla zainfekowanych plików.
c) Skanowanie załączników skompresowanych.
d) Definiowanie komunikatów powiadomień w języku polskim.
e) Blokowanie załączników w oparciu o typ pliku.
f) Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antywirusowej.
g) Moduł kontroli antywirusowej powinien mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie powinien umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
h) 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.
i) Ochronę typu wirus outbrake.

3. Kontrola antyspamowa

System powinien zapewniać poniższe funkcje i metody filtrowania spamu:

a) Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
b) Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
c) Szczegółowa kontrola nagłówka wiadomości.
d) Analiza Heurystyczna.
e) Współpraca z zewnętrznymi serwerami RBL, SURBL.
f) Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
g) Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.
h) Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.

tel. (61) 8310-142; 8310-242
email: zamowienia.publiczne@orsk.pl

i) Kontrola w oparciu o Greylisting oraz SPF.
j) Filtrowanie treści wiadomości i załączników.
k) Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
l) Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antyspamowej.
m) Ochrona typu outbrake.
n) Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
o) 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.

4. Ochrona przed atakami na usługę poczty

System powinien zapewniać poniższe funkcje i metody filtrowania:

a) Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
b) Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
c) Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
d) Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
e) Weryfikacja poprawności adresu e-mail nadawcy.

IV. FUNKCJE LOGOWANIA I RAPORTOWANIA

W tym zakresie dostarczony system ochrony poczty powinien 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.

V. FUNKCJE PRACY W TRYBIE WYSOKIEJ DOSTĘPNOŚCI (HA)

System ochrony poczty powinien 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.

VI. ANALIZACJE SYGNATUR, DOSTĘP DO BAZY SPAMU

W tym zakresie dostarczony system ochrony poczty powinien 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.

tel. (61) 8310-142; 8310-242
email: zamowienia.publiczne@orsk.pl

VII. ZARZĄDZANIE

System ochrony poczty powinien zapewniać poniższe funkcje:

1. System powinien 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 3 lokalnych kont administracyjnych.

VIII. GWARANCJA ORAZ WSPARCIE

Gwarancja: System powinien być objęty serwisem gwarancyjnym producenta przez oferowany okres miesięcy (min. 48 miesięcy), polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent powinien zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

tel. (61) 8310-142; 8310-242
email: zamowienia.publiczne@orsk.pl