Załącznik nr 1 do ogłoszenia

Szczegółowe wymagania systemu ochrony poczty elektronicznej

System ochrony poczty musi zapewniać zintegrowaną ochronę typu antivirus, antispyware, antispam, bazującą na komercyjnych bazach zabezpieczeń, bez licencyjnego limitu liczby chronionych kont użytkowników. System musi być dostarczony w modelu własnościowym. Brak wykupienia odnowienia licencji wsparcia technicznego dla rozwiązania nie skutkuje zablokowaniem funkcjonowania systemu ograniczając jedynie dostęp do aktualizacji oprogramowania.
System ochrony poczty musi być objęty serwisem producenta rozwiązania przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
W ramach systemu ochrony poczty wymagane są licencje uprawniające do korzystania przez okres 12 miesięcy z aktualnych baz funkcji ochronnych producenta oraz serwisów i muszą obejmować co najmniej: kontrolę antywirusową/antyspamową, filtrację URL, obsługę typu Sanbox, usuwanie niebezpiecznej zawartości typu Content Disarm/Reconstruction, Virus/Spam Outbrake.
Rozwiązanie musi posiadać certyfikaty:

1. Common Criteria NDPP,
2. FIPS 140-2 Certified,
3. VBSpam/VB100 rated,

oraz pochodzić od oficjalnego dystrybutora autoryzowanego do sprzedaży rozwiązania na terenie Polski.

Parametry fizyczne systemu

1. System musi być zrealizowany jako 2 dedykowane instancje wirtualne, bazujące na VMware ESX/ESXi 7.x,
2. Każda z instancji wirtualnych musi obsługiwać co najmniej 4 wirtualne interfejsy sieciowe (2 operacyjne oraz 2 zapasowe) oraz zapewniać przestrzeń dyskową o pojemności co najmniej 2 TB, umożliwiać obsługę protokołów NFS oraz iSCSI.

Wymagania trybów pracy

System ochrony poczty musi zapewniać obsługę klastra HA oraz wsparcie dla trybów pracy:

1. Gateway,
2. Transparentny gateway, niewymagający dodatkowej konfiguracji wykorzystywanego systemu poczty elektronicznej,

W trybie klastra HA, system ochrony poczty musi zapewniać:

1. Możliwość konfiguracji HA w trybach: gateway, transparent gateway
2. Możliwość synchronizacji konfiguracji dla scenariuszy, gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu,
4. Możliwość monitorowanie stanu pracy klastra.

Ogólne funkcje systemu ochrony poczty

System ochrony poczty musi zapewniać:

1. Integrację z systemami pocztowymi bazującymi na platformie Zimbra Network Edition, co najmniej w zakresie interfejsu użytkownika (zimlet umożliwiający obsługę kwarantanny) oraz ochrony poczty przychodzącej i wychodzącej,
2. Możliwość definiowania komunikatów, powiadomień w języku polskim,
3. Obsługę dla co najmniej 160 domen pocztowych per jedna wirtualna instancja rozwiązania,
4. Realizację skanowania antyspamowego i antywirusowego z wydajnością co najmniej 50 tys. wiadomości/godzinę,
5. Wsparcie dla szyfrowania komunikacji SMTP w zakresie protokołów SSL, TLS 1.0, TLS 1.1, TLS 1.2 oraz TLS 1.3.
6. Zapewniać ochrona przed wyciekiem informacji poufnej/DLP,
7. Obsługę polityk filtrowania poczty opartych co najmniej o: adresy mailowe, nazwy domenowe, adresy IP,
8. Obsługę białych i czarnych list adresów mailowych definiowane globalnie oraz z granulacją do określonych domen oraz poszczególnych użytkowników,
9. Routing poczty na bazie reguł lokalnych oraz zewnętrzny serwer LDAP,
10. Zdalne zarządzanie kolejkami wiadomości, m.in. w celu dostarczenia wiadomości zatrzymanych w kwarantannie,
11. Możliwość ograniczenia liczby wiadomości poczty kierowanych do chronionych domen w oparciu o liczbę jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie,
12. Ochronę i analizę zarówno poczty przychodzącej jak i wychodzącej.
13. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów na bazie rozwiązań typu sandbox, w tym możliwość poddania ponownemu skanowaniu wiadomości w momencie zwalniania ich z kwarantanny,
14. Możliwość tworzenia polityk kontroli antywirusowej oraz antyspamowej z uwzględnieniem użytkownika oraz atrybutów z zewnętrznego serwera LDAP,
15. Generowanie statystyk dziennych dla kwarantanny poczty
16. Możliwość samodzielnej obsługi kwarantanny przez uprawnionego użytkownika poprzez interface WWW,
17. Możliwość archiwizacji poczty przychodzącej i wychodzącej w oparciu o polityki.
18. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, obsługiwanych przez protokoły NFS, iSCSI.
19. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.

Zakres ochrony antywirusowej i antyspamowej

System ochrony poczty musi zapewniać:

1. Możliwość zdefiniowania nie mniej niż 200 polityk dla kontroli antywirusowej oraz antyspamowej każda,
2. Skanowanie antywirusowe wiadomości, załączników, załączników zaszyfrowanych, załączników skompresowanych,
3. Kwarantannę dla zainfekowanych plików,
4. Blokowanie załączników w oparciu o typ pliku,

5. Moduł kontroli antywirusowej musi mieć możliwość współpracy z komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox, w celu rozpoznawania nieznanych dotąd zagrożeń, obsługi zdarzeń typu virus outbreak,
6. Możliwość definiowania różnych akcji dla wykrytych zagrożeń, w zakresie co najmniej: oznaczania wiadomości (tag), dodawania nagłówka, zastąpienia podejrzanej treści lub załącznika, odrzucenia lub usunięcia wiadomości, przekazania do innego systemu pocztowego, powiadomienia administratora,
7. Możliwość oczyszczania wiadomości z zawartych w załącznikach zagrożeń typu makra, niebezpieczne adresy URL, skrypty, ActiveX dla plików tekstowych, PDF, HTML, MS Office/OpenOffice.
8. Możliwość definiowania maksymalnej liczby otrzymywanych i wysyłanych wiadomości w jednostce czasu,
9. Obsługę serwerów niezależnych list RBL, SURBL
10. Możliwość korzystania z komercyjnych baz reputacyjnych dla adresów źródłowych IP oraz domen,
11. Analizę wiadomości w oparciu o heustykę oraz sygnatury dostarczane komercyjne przez producenta rozwiązania,
12. Filtrowanie w oparciu o filtry Bayes'a z możliwością samoczynnej ich aktualizacji, dostrajania globalnie, dla poszczególnych chronionych domen oraz użytkowników,
13. Filtrowanie treści wiadomości, załączników oparciu o kategorie typu malware, phishing, ransomware, itd.,
14. Wykrywanie spamu poprzez analizę plików graficznych oraz PDF,
15. Kontrolę wiadomości w oparciu o SPF, DKIM, DMARC, Reverse DNS, Greylisting,
16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing), w tym na poziomie C (C-level), email-bombing,

Funkcje logowania i raportowania

System ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG,
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia przestrzeni dyskowej,
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 zagrożeń 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.

Aktualizacje sygnatur, dostęp do bazy spamu

System ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazy spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

Zarządzanie systemem

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania z wykorzystaniem protokołów: HTTPS oraz SSH,
2. Możliwość dostosowywania wyglądu interfejsu zarządzania oraz WebMail,
3. Możliwość zdefiniowania lokalnych kont administracyjnych,
4. Uwierzytelnianie użytkowników może opierać się na lokalnej bazie lub zdalnych serwerach LDAP, Radius.