***Załącznik nr 1***

**Opis Przedmiotu Zamówienia**

Przedmiotem zamówienia jest dostawa systemu do ochrony poczty elektronicznej .

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa** | **Uwagi / SKU / SN** | **ilość** |
| 1. | Proofpoint - PFPT Email Protection F-Secure | PP-B-EPT-V-E-104 | 1700 |
| 2. | Proofpoint - PFPT Platinum Level Support | PP-SUP-PS-12 | 1 |
| 3. | Proofpoint - PFPT Threat Response Auto-Pull - V - mSOAR | PP-M-AP-V-C-104 | 1700 |
|  | Usługa wdrożenia systemu system do ochrony poczty elektronicznej wraz z instruktarzem z administracji systemem dla 3 osób |  | 1 |
| 4. | Usługa wsparcia partnera producenta systemu |  | 1 |

System będzie instalowany na środowisku zamawiającego VMware vSphere. Zamawiający zapewni niezbędne środowisko serwerowe zawierające systemy operacyjne i inne niezbędne oprogramowanie wskazane przez Wykonawcę .

**Wymagania funkcjonalne dla systemu do ochrony poczty elektronicznej.**

1. System musi zapewniać ochronę przed zagrożeniami związanymi z przesyłaniem poczty elektronicznej (wirusy, spam, phishing, niedozwolone treści, etc.).
2. System musi być dostarczony w postaci zamkniętego rozwiązania sprzętowego lub obrazu maszyny wirtualnej kompatybilnego z VMWare vSphere lub Microsoft Hyper-V.
3. Zarządzanie lokalne i zdalne systemem musi być możliwe przy użyciu bezpiecznego połączenia HTTPS przez przeglądarkę internetową oraz poprzez protokół SSH.
4. System musi umożliwiać pracę w architekturze nadmiarowej Master-Agent z możliwością przypisania profili funkcyjnych (filtrowania wiadomości, bazy kwarantanny, serwera logów) poszczególnym agentom.
5. System musi pracować jako brama SMTP i być niezależnym od rodzaju stosowanego, chronionego serwera poczty.
6. System musi umożliwiać filtrowanie poczty przychodzącej dla wskazanych domen oraz przesyłanie ruchu pocztowego na wskazane serwery pocztowe.
7. System musi umożliwiać filtrowanie poczty wychodzącej do wskazanych przez Administratora serwerów pocztowych/domen.
8. System musi zapewnić możliwość zdefiniowania osobnych tras przesyłania poczty dla ruchu przychodzącego i wychodzącego w oparciu o statyczne wpisy adresów serwerów, smart hosta lub rekordy MX serwerów DNS.
9. Administrator musi mieć możliwość zapisu konfiguracji na zewnętrzny nośnik i odtworzenia zapisanej wcześniej konfiguracji.
10. System musi umożliwiać automatyczne wykonywanie kopii zapasowej konfiguracji zgodnie z harmonogramem.
11. System w momencie dostarczenia lub po odtworzeniu musi zawierać zestaw predefiniowanych reguł i polityk dla wszystkich modułów filtrujących: AV, antyspam, kontrola treści.
12. System musi umożliwiać automatyczne pobieranie oraz instalowanie aktualizacji modułów ochronnych oraz całego systemu.
13. Wszystkie aktualizacje muszą być pobierane z jednego miejsca a system musi komunikować się ze źródłem aktualizacji z częstotliwością narzuconą przez administratora systemu.
14. System musi zapewnić śledzenie historii wykonywania aktualizacji.
15. Producent musi zapewnić możliwość zakupu aktualizacji systemu jednorazowo na okres roku, dwóch lub trzech lat.
16. System musi umożliwiać tworzenie wielu administratorów oraz przypisanie im odpowiednich uprawnień dostępowych do modułów ochronnych.
17. System musi zapewniać rozbudowany system raportowania zapewniający dostęp do minimum 40 różnych rodzajów graficznych raportów oraz musi mieć możliwość tworzenia własnych raportów.
18. System w momencie dostarczenia lub po odtworzeniu musi zawierać zestaw predefiniowanych raportów.
19. Administrator musi mieć możliwość okresowej publikacji wybranych raportów jako strony WWW lub przy pomocy wysyłanych automatycznie wiadomości email.
20. System musi umożliwiać eksport logów do formatu CSV oraz XML.
21. System musi umożliwiać logowanie na lokalnym dysku twardym lub zewnętrznym serwerze Syslog zdarzeń podejmowanych przez filtry oraz zdarzeń dotyczących komunikacji SMTP.
22. System musi posiadać lokalną kwarantannę dla zainfekowanych wiadomości.
23. System musi zapewniać użytkownikom końcowymi możliwość zarządzania wiadomościami trafiającymi do ich personalnej kwarantanny.
24. System musi umożliwiać określanie poziomu dostępu i akcji możliwych do wykonania w obrębie kwarantanny dla różnych użytkowników/grup użytkowników.
25. Kwarantanna użytkownika oraz skrócone informacje o stanie kwarantanny dla użytkownika muszą być dostępne w języku polskim.
26. System musi zapewniać możliwość uwierzytelniania użytkownika w celu zmian parametrów własnego folderu kwarantanny. W tym celu, system musi wspierać mechanizmy uwierzytelnienia jednokrotnego (Single Sign-On) oparte o usługi federacyjne domeny Active Directory (ADFS) lub protokół SAML 2.0.
27. System musi zapewniać możliwość definiowania list zaufanych i blokowanych nadawców przez użytkowników końcowych.
28. System musi umożliwiać definiowanie wyglądu kwarantanny końcowego użytkownika zarówno, co do jej szaty graficznej (np. możliwość umieszczenia znaku firmowego) jak i treści komunikatów.
29. System musi umożliwiać definiowanie i przeglądanie wielu katalogów kwarantanny dla różnych reguł antywirusowych i antyspamowych.
30. Dla wszystkich stworzonych folderów kwarantanny system musi zapewniać możliwość ustawienia maksymalnego czasu przechowywania wiadomości a po jego upływie automatycznie je usuwać.
31. System musi umożliwiać wyszukiwanie wiadomości w kwarantannie na podstawie nadawcy, odbiorcy, tematu wiadomości lub czasu od kiedy wiadomość znajduje się w kwarantannie.
32. System musi umożliwiać następujące operacje na wiadomościach przechowywanych w obszarze kwarantanny: usunięcie wiadomości, przesłanie do innego odbiorcy, przeniesienie do innego folderu, zwolnienie wiadomości, zwolnienie zaszyfrowanej wiadomości.
33. System musi zapewniać możliwość zgłoszenia przypadków złej klasyfikacji wiadomości do producenta systemu na poziomie kwarantanny administratora oraz personalnej kwarantanny użytkownika końcowego.
34. System musi umożliwiać tworzenie listy użytkowników zdefiniowanych lokalnie, a także zapewniać możliwość importu użytkowników z serwerów: Active Directory, Azure Active Directory, LDAP, MS Exchange, Lotus Domino lub za pomocą odpowiednio przygotowanych plików (tekstowych, csv).
35. System musi zapewniać możliwość ustawienia przez administratora harmonogramu importowania użytkowników.
36. System musi zapewniać możliwość tworzenia grup użytkowników oraz przypisywania im odpowiedniej konfiguracji, przynajmniej w zakresie: wykorzystywanych polityk filtrowania wiadomości, metody dostępu do personalnej kwarantanny, język kwarantanny, szata graficzna kwarantanny, źródło uwierzytelniania.
37. System musi umożliwiać konfigurację harmonogramu wysyłania powiadomień mailowych do użytkowników o np. nowych wiadomościach zatrzymanych w kwarantannie.
38. System musi posiadać graficzny interfejs administratora do śledzenia wiadomości na poziomie modułu MTA i modułach filtrujących na podstawie parametrów:

* odbiorca,
* nadawca,
* nazwa załącznika,
* temat wiadomości,
* sender hostname lub IP,
* QID,
* RuleID,
* Message ID,
* nazwa wirusa,
* SID.

1. System musi zapewniać możliwość tworzenia własnych reguł filtrowania treści w oparciu o:

* adresy IP nadawców odbiorców,
* adresy email,
* typ i rozmiar załącznika,
* ilość załączników,
* treść maila,
* pola nagłówka wiadomości,
* treść załączników.

1. System musi umożliwiać tworzenie własnych reguł filtrowania lub klonowania istniejących.
2. System musi umożliwiać tworzenie słowników słów kluczowych.
3. System musi zapewniać mechanizm weryfikacji poprawności nazwy odbiorcy na podstawie zapytań serwera LDAP, SMTP lub lokalnego repozytorium użytkowników.
4. System musi zapewniać wsparcie dla standardu Sender Policy Framework (SPF).
5. System musi zapewniać wsparcie dla standardu Domain Keys Identified Mail (DKIM).
6. System musi zapewniać wsparcie dla standardu Domain-based Message Authentication Reporting & Conformance (DMARC).
7. Ochrona antywirusowa musi być realizowana poprzez silniki zasilane w sygnatury oraz filtr analizy heurystycznej wykrywający ataki typu zero hour.
8. System musi umożliwiać przegląd ostatnich infekcji oraz listę najczęstszych wykrytych zagrożeń.
9. Aktualizacje sygnatur modułu antywirusowego muszą być dostępne nie rzadziej niż raz na dobę.
10. System musi zapewniać możliwość tworzenia wielu polityk ochrony antywirusowej przydzielanych w oparciu o: adresy IP serwera nadawcy, adres email nadawcy/odbiorcy wiadomości.
11. System musi zapewniać możliwość definiowania różnych sposobów postępowania z zainfekowanymi wiadomościami w zależności od rodzaju wykrytego wirusa.
12. System musi zapewniać możliwość określenia postępowania z zabezpieczonymi wiadomościami (załączniki chronione hasłem, podpisane wiadomości, etc.).
13. Moduł detekcji spamu musi bazować na metodzie zaawansowanej analizy heurystycznej, która wyklucza konieczność ręcznego tworzenia reguł w razie pojawienia się nowych technik omijania filtrów antyspamowych.
14. System musi umożliwiać korzystanie ze źródeł producenta, niepublicznych serwerów badania reputacji nadawców maila.
15. System musi zapewniać możliwość automatycznej oceny reputacji źródła przesyłanego maila (na podstawie weryfikacji ilości połączeń, procentowej ilości maili z wirusami, procentowej ilości wiadomości sklasyfikowanych jako spam) z możliwością limitowania ilości odbieranych wiadomości w określonej jednostce czasu od źródeł o niskiej reputacji.
16. System musi zapewniać możliwość definiowania reguł antyspamowych na poziomie całego systemu, grup użytkowników oraz pojedynczych użytkowników.
17. System musi zapewniać możliwość tworzenia list bezpiecznych i blokowanych odbiorców, nadawców, domen lub adresów IP.
18. System musi zapewniać inteligentne rozpoznawanie typów analizowanych załączników. Zmiana rozszerzeń powinna być ignorowana przez system i nie powinna być metodą omijania tego typu filtra.
19. System musi zapewniać ochronę przeciwko atakom typu Odmowa dostępu do usługi (Denial Of Service) oraz wykrywać i blokować próby enumeracji kont użytkowników chronionej domeny pocztowej (Directory Harvesting Attack).
20. System musi posiadać mechanizm ochrony przed zjawiskiem wykorzystania wiadomości niedostarczonych (Fake NDR – Non-Delivery Receipt) za pomocą cyfrowego oznaczenia wiadomości wysyłanych z chronionych domen organizacji).
21. System musi zapewniać możliwość szyfrowania przesyłek za pomocą protokołu Transport Layer Security.
22. W celu wzmocnienia mechanizmów analitycznych systemu ochrony poczty elektronicznej oraz umożliwiania podjęcia automatycznych reakcji na wykryte zagrożenia, system musi zapewniać integrację z systemem klasy SOAR. Reakcje (działania naprawcze) podejmowane przez system SOAR muszą obejmować przynajmniej możliwość automatycznego usunięcia niebezpiecznych wiadomości dostarczonych na skrzynki odbiorcze użytkowników. System SOAR musi być kompatybilny przynajmniej ze środowiskiem Microsoft Exchange, Microsoft Office 365 i IBM Domino.
23. Wskazanie niebezpiecznych wiadomości – do usunięcia przez system SOAR – musi odbywać się w następstwie zgłoszenia wiadomości przez użytkownika przy użyciu wtyczki alarmującej, dostarczanej jako add-in dla oprogramowania klienta poczty elektronicznej Microsoft Outlook lub w wyniku przesłania jej kopii na monitorowaną przez system SOAR skrzynkę pocztową (tzw. abuse mailbox). Operacja usunięcia wiadomości ze skrzynki odbiorczej użytkownika musi być odwracalna, tzn. musi istnieć możliwość przywrócenia usuniętych wiadomości, np. w przypadku wystąpienia błędów typu false-positive. System SOAR musi zapewniać możliwość powiadomienia użytkownika o usunięciu wiadomości z jego skrzynki odbiorczej, jak również o jej przywróceniu. Powiadomienie musi mieć formę personalizowanej co do treści oraz wyglądu wiadomości email.
24. Zamawiający wymaga dostarczenia systemu SOAR wraz systemem ochrony poczty elektronicznej.

**Wdrożenie:**

1. Instalacja zaoferowanego systemu
2. Konfiguracja podstawowych polityk wraz z zastosowaniem dobrych praktyk
3. Uruchomienie SPF
4. Uruchomienie DKIM
5. Przeniesienie do wdrażanego systemu obecnych blacklist i whitelist z dotychczasowego systemu
6. Analiza obecnych polityk antyspamowych i w razie potrzeby skonfigurowanie analogicznych na nowym systemie
7. Przygotowanie dokumentacji powykonawczej wraz z procedurami usuwania najczęstszych problemów, backupu, odzyskania środowiska po awarii.
8. Przeprowadzenie instruktażu dla 3 Administratorów Zamawiającego trwającego min. 3 dni roboczych każdy po 8 godzin, gdzie 50% czasu będzie poświęcone na ćwiczenia praktyczne.

**Wsparcie techniczne**

Dodatkowo wymagane jest wsparcie partnera producenta systemu w zakresie rozwiązywania problemów z działaniem systemu, patchowaniem i rozwojem systemu (proponowanie i uruchamianie nowych funkcjonalności – rozwój systemu) min. jeden dzień roboczy w miesiącu (8 godzin)- 12 dni w roku.