*Załącznik nr 2 – formularz ofertowy techniczny – część nr 2*

*Zakup specjalistycznego oprogramowania oraz sprzętu w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych wykorzystywanych w Szpitalu (sygnatura: ZP/2501/104/22)*

*Uwaga: Wykonawca zostaje zobowiązany do uzupełnienia kolumny „Oferowane parametry” o opis spełnienia wymaganych minimalnych parametrów technicznych. Zamawiający wymaga ponadto, aby* ***przedmiotowe środki dowodowe, złożone wraz z ofertą,*** *potwierdziły sporządzony przez wykonawcę opis.*

**2. Antyspam**

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Element konfiguracji** | **Wymagane minimalne parametry techniczne** | **Oferowane parametry**  **(wymagany opis)** |
| 1. | Wymagania ogólne systemu | 1. Licencja musi umożliwiać działanie systemu dla min 250 aktywnych użytkowników posiadających pojedynczy adres e-mail przez okres min.3lat .  2. System musi posiadać konsolę zarządzającą dostępną przez przeglądarkę internetową.  3. System musi umożliwiać dostęp do konsoli osobno poprzez http oraz https  4. System musi mieć możliwość implementacji wewnątrz i na zewnątrz struktury informatycznej organizacji, powinien funkcjonować niezależnie od pozostałych jej elementów.  5. Rozwiązanie musi wspierać filtrację dla serwerów znajdujących się wewnątrz i na zewnątrz struktury informatycznej danej organizacji.  6. System musi być dostępny w postaci pliku ISO pozwalającym na instalację na serwerze fizycznym, jak też w wersji na maszyny wirtualne ze wsparciem dla następujących środowisk: VMWare, Citrix, MS Hyper-V.  7. Interfejs rozwiązania musi wspierać kilka języków i posiadać także polskojęzyczny interfejs.  8. System musi zawierać główny pulpit, na którym będą wyświetlane podstawowe informacje takie jak:  a. Stan systemu w tym zużycie CPU, RAM, pamięci dyskowej  b. Wersję systemu i bieżącą datę  c. Informacje o typie aktualnie używanego procesora  d. Informacje o stanie skanerów antywirusowych  e. Wykres przedstawiający informacje zbiorcze na temat procesowania wiadomości  f. Informacje z ostatnich siedmiu dni w formie listy lub/i wykresu przedstawiające liczbę zablokowanych wiadomości, liczbę wystąpień wirusów, liczbę zablokowanych załączników i innych odrzuceń  g. Listy najpopularniejszych nadawców wirusów i spamu oraz najpopularniejszych wirusów wykrytych przez silniki antywirusowe  9. System musi w widocznym miejscu zawierać sekcje poświęconą wsparciu technicznemu umożliwiającą utworzenie bezpiecznego połączenia z suportem producenta.  10. Konsola zarządzająca musi mieć możliwość dostosowywania wyglądu, personalizacji kolorystyki interfejsu i umieszczenia logo firmy.  11. System musi mieć możliwość obsługi certyfikatów SSL.  12. System musi mieć możliwość importu certyfikatów.  13. System musi mieć możliwość obsługi TLS.  14. System musi mieć funkcjonalność szyfrowania emaili kluczem prywatnym, i odszyfrowywania ich u odbiorcy kluczem publicznym, tak zwane DKIM  15. System musi mieć możliwość uwierzytelniania nadawcy poprzez określone mechanizmy, nie mniej niż SPF, DMARC, ARC.  16. System musi mieć możliwość wykonywania kopii zapasowych konfiguracji zarówno automatycznych na serwerze FTP lub w chmurze, jak i na żądanie, a także możliwość importu takiej konfiguracji.  17. System musi obsługiwać zdalny Syslog, osobny dla logów dotyczących maili i osobny dla logów dotyczących inferface’u oraz zmian w systemie  18. System musi wspierać SNMP v2c oraz v3  19. System musi mieć możliwość pracy w klastrze (dwóch lub więcej węzłów).  20. Aktualizacja systemu musi odbywać się poprzez konsolę webową, oraz nie może mieć wpływu na działanie samego systemu (tj. żadna wiadomość mailowa nie zostanie utracona). W przypadku aktualizacji systemów działających w klastrze, musi istnieć możliwość uruchomienia tych procesów oddzielnie (np. w przypadku gdyby aktualizacja okazała się wadliwa) |  |
| 2. | Moduł antyspamowy | 1. System musi posiadać wbudowany silnik antyspamowy.  2. System musi mieć umożliwiać korzystanie z zewnętrznych baz RBL, dowolnie definiowanych przez administratora.  3. System musi mieć możliwość tworzenia przez administratora białej listy adresów IP nadawcy, pomijanych podczas filtracji RBL.  4. System musi mieć możliwość wyłączania filtracji RBL dla poszczególnych domen podpiętych do rozwiązania.  5. System musi mieć możliwość sprawdzenia poprawności odbiorcy danej wiadomości, w trybie co najmniej: dynamicznym (weryfikacja na serwerze docelowym), LDAP, listę dozwolonych odbiorców oraz poprzez wyrażenia regularne.  6. System musi być wspierany samouczącą się bazą danych Bayes’a.  7. System musi obsługiwać Passive OS Fingerprinting oraz mechanizm Penpals i analizę Botnetów.  8. System musi posiadać konfigurowalną szarą listę, z możliwością jej włączenia i wyłączenia  9. System musi pozwalać na zdefiniowanie języków, w których to muszą być napisane wiadomości, by pomyślnie przeszły weryfikację  10. System musi umożliwiać tworzenie białych i czarnych list, opartych na adresach email oraz nazwach domen. Listy powinny być traktowane globalnie, per domena i osobno dla każdego użytkownika.  11. System musi umożliwiać tworzenie białych i czarnych list, opartych na adresach IP serwerów pocztowych nadawcy.  12. System musi mieć możliwość indywidualnego ustalania wysokości progu filtrowania wiadomości przez moduł antyspamowy dla domen jak i również dla określonych aliasów pocztowych.  13. System musi mieć możliwość rozczytywania skróconych wersji URLi  14. System musi mieć możliwość dodawania konfigurowalnych stopek do maili wychodzących, które potwierdzą że zostały one przefiltrowane przez tenże system |  |
| 3. | Moduł antywirusowy | 1. System musi zawierać dwa niezależnie działające silniki antywirusowe zewnętrznego dostawcy.  2. System musi mieć możliwość całkowitego wyłączenia silnika antywirusowego.  3. System musi samoczynnie aktualizować bazę danych dla wbudowanego silnika antywirusowego. Baza musi być aktualizowana minimum, co godzinę. |  |
| 4. | Moduł kontroli treści | 1. System musi umożliwiać blokowanie wybranych przez administratora rozszerzeń i nazw plików.  2. System musi umożliwiać blokowanie co najmniej następujących rozszerzeń plików:  ade, adp, bat, chm, cmd, com, cpl, dll, doc, exe, hta, ins, isp, jar, js, jse, lib, lnk, mde, msc, msp, mst, pif, scr, sct, shb, sys, vb, vbe, vbs, vxd, wsc, wsf, wsh   1. System musi umożliwiać blokowanie co najmniej następujących typów MIME:   application/ecmascript, application/javascript, application/x-javascript,  application/x-msdos-program, application/x-msdownload, text/ecmascript,  text/javascript  4. Wykrywanie i blokowanie rozszerzenia załącznika typu wykonywalnego powinno być odporne na zmianę nazwy i rozszerzenia, również w przypadku skompresowanego archiwum.  5. System musi umożliwiać blokowanie zabezpieczonych hasłem archiwów.  6. System musi umożliwiać tworzenie własnych reguł filtracji.  7. System musi umożliwiać kontrolę treści opartej na słowniku lub wyrażeniu regularnym (przykładowo blokowanie wiadomości z numerami kard kredytowych, numerami PESEL czy też innymi danymi określanymi jako wrażliwe).  8. Wszystkie wyżej wymienione funkcje powinny być dostępne dla filtracji wiadomości wychodzących i przychodzących.  9. System musi posiadać mechanizm przepisywania linków w wiadomościach, automatycznie kierujący odbiorcę na serwery zewnętrzne, które kategoryzują strony internetowe pod kątem zagrożeń:  a. Funkcjonalność można ustawić osobno dla domeny i dla użytkownika systemu  b. Można tworzyć wyjątki dla domen stron internetowych, które mają być nie przepisywane, osobno dla całej domeny pocztowej oraz użytkowników systemu.  c. Funkcjonalność powinna pozwalać na edycję wyświetlanej strony z informacją o blokadzie, minimum o treść wyświetlanej informacji oraz o wyświetlane logo. |  |
| 5. | Kwarantanna | 1. System musi posiadać mechanizm kwarantanny.  2. System musi zawierać wbudowaną wyszukiwarkę.  3. System musi generować raporty kwarantanny  a. Raporty kwarantanny powinny być generowane automatycznie lub na żądanie  b. Raporty kwarantanny powinny być personalizowane (w tym podmiana logo producenta)  c. Raporty powinny być generowane dla użytkowników systemu pocztowego.  d. W przypadku współpracy z serwerami pocztowymi Microsoft Exchange, raport powinien być generowany dla użytkownika tylko raz, uwzględniając jego wszystkie aliasy.  4. System musi umożliwić dostęp do kwarantanny poprzez interfejs przeglądarki internetowej dla każdego użytkownika indywidualnie z możliwością dopasowania odpowiednich uprawnień.  5. System musi umożliwić uwierzytelnianie użytkownika za pośrednictwem wewnętrznej bazy, LDAP, w oparciu o bazę kont na docelowym serwerze pocztowym (POP3, IMAP), lub bazy SQL. |  |
| 6. | Pozostałe funkcjonalności | 1. System musi mieć możliwość tworzenie wielu administratorów o zróżnicowanym poziomie uprawnień.  2. System musi mieć możliwość tworzenia grup domen przyporządkowanych odpowiednim administratorom.  3. System musi posiadać funkcję kontroli ilości przetwarzanych wiadomości dla ruchu przychodzącego i wychodzącego.  4. System musi umożliwiać wyświetlanie statystyk dotyczących aktualnego użycia licencji (liczby unikalnych kont mailowych, przez które przechodzą wiadomości).  5. System musi umożliwiać manualne ustawienie równocześnie pracujących procesów SMTP w celu optymalizacji wydajności rozwiązania względem platformy, na której jest zainstalowane.  6. System musi posiadać moduł kontroli jakości, który pozwoli zdefiniować ograniczenia odnoszące się do co najmniej:  a. ilości maili, które mogą zostać wysłane z określonej jednostce czasu  b. zbiorczego rozmiaru maili, które mogą zostać wysłane w określonej jednostce czasu  7. System musi mieć możliwość ujednolicenia aliasów emailowych  8. System powinien mieć możliwość konfiguracji raportów generowanych użytkownikom tak, aby mogły być generowane na żądanie (z opcją wyłączenia tej opcji przez administratora). |  |
| 7. | Serwisy i licencje | Wsparcie: System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego.  W ramach usług wynikających z udzielonej gwarancji jakości oraz technicznego Wykonawca zapewnia:   1. udostępnienie poprawek do Oprogramowania Aplikacyjnego, w przypadku stwierdzenia przez Zamawiającego błędu Oprogramowania Aplikacyjnego: 2. w przypadku tzw. błędu krytycznego, tj. takiego, który uniemożliwia użytkowanie Oprogramowania Aplikacyjnego (w zakresie jego podstawowej funkcjonalności wskazanej w dokumentacji użytkownika) i prowadzi do zatrzymania jego eksploatacji, utraty danych lub naruszenia ich spójności, w wyniku których niemożliwe jest prowadzenie działalności z użyciem Oprogramowania Aplikacyjnego:    * + 1. reakcja Wykonawcy na zgłoszenie Zamawiającego (tj. czas od otrzymania zgłoszenia do chwili podjęcia przez Wykonawcę czynności zmierzających do naprawy zgłoszonego „błędu krytycznego”) 1 dzień roboczy;        2. czas dokonania i udostępnienia Zamawiającemu odpowiednich korekt Oprogramowania Aplikacyjnego wyniesie do 3 dni roboczych od chwili rozpoczęcia czynności serwisowych;        3. w przypadku wystąpienia „błędu krytycznego”, Wykonawca, po uzyskaniu od Zamawiającego zgody, może wprowadzić tzw. rozwiązanie tymczasowe, doraźnie rozwiązujące problem błędu krytycznego; w takim przypadku dalsza obsługa usunięcia dotychczasowego błędu krytycznego będzie traktowana jako błąd zwykły; 3. w pozostałych przypadkach, określanych jako „błędy zwykłe” - błędy Oprogramowania Aplikacyjnego inne niż błędy krytyczne:    * + 1. czas reakcji Wykonawcy na zgłoszenie Zamawiającego (tj. czas od otrzymania zgłoszenia do chwili podjęcia przez Wykonawcę czynności zmierzających do naprawy zgłoszonego błędu zwykłego) wynosi do 15 dni roboczych;        2. czas dokonania i udostępnienia Zamawiającemu odpowiednich korekt Oprogramowania Aplikacyjnego wyniesie do 60 dni roboczych od chwili rozpoczęcia czynności serwisowych; |  |

|  |  |
| --- | --- |
| miejscowość: |  |
| data: |  |

(podpis pieczątka imienna osoby upoważnionej

do składania oświadczeń woli w imieniu Wykonawcy)