**Załącznik nr 2 do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**DOSTAWA INFRASTRUKTURY SPRZĘTOWEJ ORAZ OPROGRAMOWANIA**

Przedmiotem zamówienia jest dostawa sprzętu i oprogramowania podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych w „Kutnowskim Szpitalu Samorządowym” Sp. z o.o.

Poniżej wyspecyfikowano minimalne parametry sprzętu oraz oprogramowania, które należy dostarczyć w ramach realizacji przedmiotu zamówienia. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna.

Wymagania ogólne:

* Całość dostarczanego sprzętu i oprogramowania standardowego musi pochodzić z autoryzowanego kanału sprzedaży producenta.
* Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu, producenta, jak i daty produkcji danego elementu.
* Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
* Do każdego urządzenia musi być dostarczony niezbędny sprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe itp.) niezbędny do uruchomienia danego urządzenia w budowanym rozwiązaniu w miejscu dostawy wskazanym przez Zamawiającego. Sprzęt, o którym mowa powyżej jest integralną częścią oferty i przechodzi na własność Zamawiającego.
* Wszystkie urządzenia muszą posiadać oznakowanie CE.
* Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL)
* Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.
* Wymagane jest, aby infrastruktura sprzętowa była gotowym produktem posiadającym nazwę handlową i złożonym z zamkniętej, ściśle zdefiniowanej listy komponentów posiadających odpowiednie numery katalogowe.
* Dostarczane oprogramowanie musi zostać dostarczone w najnowszej stabilnej wersji, która uzyskała certyfikację producenta dostarczanego sprzętu (jeśli podlega certyfikacji).

Zamawiający wymaga aby Wykonawca realizując opisane w przedmiocie zamówienia dostawy i usługi uwzględnił uwarunkowania środowiska aktualnie pracującego u Zamawiającego, w szczególności uwzględniając:

* posiadane środowisko domenowe,
* posiadaną konfigurację sieci wraz z jednostkami podległymi,
* posiadaną konfiguracją baz danych i backupów,
* konfigurację stacji roboczych.

Wykonawca po zainstalowaniu i skonfigurowaniu sprzętu i oprogramowania będzie miał obowiązek przeprowadzenia instruktażu dla administratorów Zamawiającego w zakresie konfiguracji i zarządzania **dostarczonego sprzętu oraz oprogramowania.**

1. **Rozwój systemu kopii bezpieczeństwa przez:**
2. Rozbudowę biblioteki taśmowej TS4300 :
* dodatkowy napęd LTO-7 HH
* 20 taśm LTO-7
* Wydłużenie serwisu o 24 miesiące
1. Serwer testowania kopii zapasowych oraz testowych odtworzeni kopii:

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Wymagane minimalne parametry techniczne | Wymóg do spełnienia (warunek graniczny) | OFEROWANE PARAMETRY TECHNICZNE – podaje WykonawcaWymogi dotyczące opisu oferowanych parametrów:TAK – wykonawca spełnia konkretny parametr przy czym Zamawiający oczekuje by w przypadku wymagań dotyczących minimalnych parametrów opisać szczegółowo parametry oferowane przez wykonawcęNIE – wykonawca nie spełnia konkretnego parametru |
|  | Obudowa do montażu w szafie typu rack | TAK |  |
|  | Zasilanie redundantne, przynajmniej 2 zasilacze typu HotPlug | TAK |  |
|  | Płyta główna z możliwością zainstalowania minimum dwóch procesorów | TAK |  |
|  | Zegar procesora minimum 2,7 GHz | TAK |  |
|  | Zainstalowany min 1 procesor minimum dziesięciordzeniowy klasy x86 dedykowane do pracy w serwerach, zaprojektowane do pracy w układach wieloprocesorowych | TAK |  |
|  | Pamięć minimum 128GB ECC DIMM, rozszerzalna, z zabezpieczeniem typu: ECC | TAK |  |
|  | Dyski minimum 2x 960GB SSD skonfigurowane w RAID1, 2x1,92TB SSD skonfigurowane w RAID1 , 8x18TB 7.2K | TAK |  |
|  | Sieć minimum 2x16Gb FC, 2x10Gb SFP+ SR | TAK |  |
|  | Z przodu obudowy: 1x USB 3.0, 1x USB 2.0 | TAK |  |
|  | Z tyłu obudowy: 2x USB 3.0, , 1x DB-15 | TAK |  |
|  | Zarządzanie:* Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania
* Monitoring statusu i zdrowia systemu
* Logowanie zdarzeń
* Umożliwiający Update systemowego firmware
* Umożliwiający zdalną konfigurację serwera
* Monitoring i możliwość ograniczenia poboru prądu
* Zdalne włączanie/wyłączanie/restart
* Przekierowanie konsoli szeregowej przez IPMI
* Zrzut ekranu w momencie zawieszenia system
* Możliwość przejęcia zdalnego ekranu 1920x1200, 60 Hz,16 bpp
* Zdalny dostęp do serwera
* Możliwość zdalnej instalacji systemu operacyjnego
* Alerty Syslog
* Przekierowanie konsoli szeregowej przez SSH
* Wyświetlanie danych aktualnych I historycznych dla użycia energii I temperatury serwera
* Możliwość mapowania obrazów ISO z lokalnego dysku operatora
* Możliwość mapowania obrazów ISO przez HTTPS
* Możliwość jednoczesnej pracy użytkowników przez wirtualną konsolę
* Wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3
 | TAK |  |
|  | Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID | TAK |  |
|  | Serwerowy system operacyjny umożliwiający uruchomienie 2 ose oraz integrację z ActiveDirectory | TAK |  |
|  | gwarancja: min. 60 m-cy, 3YNBD, producenta  | TAK |  |

1. Rozszerzenie Systemu kopii zapasowych:

- rozszerzenie wsparcia o 36 miesięcy na posiadany przez zamawiającego system backupu Veeam Backup & Replication Enterprise

1. **Rozwój systemu bezpieczeństwa poczty:**

Wymagania ogólne systemu

1. System musi posiadać konsolę zarządzającą dostępną przez przeglądarkę internetową.
2. System musi umożliwiać dostęp do konsoli osobno poprzez http oraz https
3. System musi mieć możliwość implementacji wewnątrz i na zewnątrz struktury informatycznej organizacji, powinien funkcjonować niezależnie od pozostałych jej elementów.
4. Rozwiązanie musi wspierać filtrację dla serwerów znajdujących się wewnątrz i na zewnątrz struktury informatycznej danej organizacji.
5. 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.
6. Interfejs rozwiązania musi wspierać kilka języków i posiadać także polskojęzyczny interfejs.
7. System musi zawierać główny pulpit, na którym będą wyświetlane podstawowe informacje takie jak:
	1. Stan systemu w tym zużycie CPU, RAM, pamięci dyskowej
	2. Wersję systemu i bieżącą datę
	3. Informacje o typie aktualnie używanego procesora
	4. Informacje o stanie skanerów antywirusowych
	5. Wykres przedstawiający informacje zbiorcze na temat procesowania wiadomości
	6. Informacje z ostatnich siedmiu dni w formie listy lub/i wykresu przedstawiające liczbę zablokowanych wiadomości, liczbę wystąpień wirusów, liczbę zablokowanych załączników i innych odrzuceń
	7. Listy najpopularniejszych nadawców wirusów i spamu oraz najpopularniejszych wirusów wykrytych przez silniki antywirusowe
8. System musi w widocznym miejscu zawierać sekcje poświęconą wsparciu technicznemu umożliwiającą utworzenie bezpiecznego połączenia z suportem producenta.
9. Konsola zarządzająca musi mieć możliwość dostosowywania wyglądu, personalizacji kolorystyki interfejsu i umieszczenia logo firmy.
10. System musi mieć możliwość obsługi certyfikatów SSL.
11. System musi mieć możliwość importu certyfikatów.
12. System musi mieć możliwość obsługi TLS.
13. System musi mieć funkcjonalność szyfrowania emaili kluczem prywatnym, i odszyfrowywania ich u odbiorcy kluczem publicznym, tak zwane DKIM
14. System musi mieć możliwość uwierzytelniania nadawcy poprzez określone mechanizmy, nie mniej niż SPF, DMARC, ARC.
15. System musi mieć możliwość wykonywania kopii zapasowych konfiguracji zarówno automatycznych na serwerze FTP lub w chmurze amazona, jak i na żądanie, a także możliwość importu takiej konfiguracji.
16. System musi obsługiwać zdalny Syslog, osobny dla logów dotyczących maili i osobny dla logów dotyczących inferface’u oraz zmian w systemie
17. System musi wspierać SNMP v2c oraz v3
18. System musi mieć możliwość pracy w klastrze (dwóch lub więcej węzłów).
19. 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)

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

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.

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

1. Wykrywanie i blokowanie rozszerzenia załącznika typu wykonywalnego powinno być odporne na zmianę nazwy i rozszerzenia, również w przypadku skompresowanego archiwum.
2. System musi umożliwiać blokowanie zabezpieczonych hasłem archiwów.
3. System musi umożliwiać tworzenie własnych reguł filtracji.
4. 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).
5. Wszystkie wyżej wymienione funkcje powinny być dostępne dla filtracji wiadomości wychodzących i przychodzących.
6. System musi posiadać mechanizm przepisywania linków w wiadomościach, automatycznie kierujący odbiorcę na serwery zewnętrzne, które kategoryzują strony internetowe pod kątem zagrożeń:
	1. Funkcjonalność można ustawić osobno dla domeny i dla użytkownika systemu
	2. Można tworzyć wyjątki dla domen stron internetowych, które mają być nie przepisywane, osobno dla całej domeny pocztowej oraz użytkowników systemu.
	3. Funkcjonalność powinna pozwalać na edycję wyświetlanej strony z informacją o blokadzie, minimum o treść wyświetlanej informacji oraz o wyświetlane logo.

Moduł powiadamiania użytkowników

1. System musi posiadać moduł powiadamiający adresata bądź odbiorcę wiadomości o podjętych przez system akcjach.
2. System musi powiadamiać o zablokowanych wiadomościach w tym wiadomościach zablokowanych przez moduł antyspamowy, antywirusowy czy moduł kontroli treści.
3. Wiadomości powinny być edytowalne i wysyłane do odbiorcy lub/i nadawcy.

Kwarantanna

1. System musi posiadać mechanizm kwarantanny.
2. System musi zawierać wbudowaną wyszukiwarkę.
3. System musi generować raporty kwarantanny
	1. Raporty kwarantanny powinny być generowane automatycznie lub na żądanie
	2. Raporty kwarantanny powinny być personalizowane (w tym podmiana logo producenta)
	3. Raporty powinny być generowane dla użytkowników systemu pocztowego.
	4. 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.

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:
	1. ilości maili, które mogą zostać wysłane z określonej jednostce czasu
	2. 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)
9. Dostarczony system musi zostać zainstalowany dla 250 użytkowników Zamawiającego
10. Okres aktualizacji minimum 3 lata.

**3. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów programowych dla posiadanego przez Zamawiającego UTM Fortigate**

1. W ramach postępowania powinny zostać dostarczone tokeny programowe w ilości co najmniej 50 zgodne z posiadanym przez Zamawiającego urządzeniem FortiGate, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów oraz w ramach połączeń VPN typu client-to-site.
2. Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android,
3. Dla tokenów na system iOS i Android wymaga się:
4. aktywacji z systemu firewall FortiGate
5. generowania kodu (cyfr) co 30 lub 60 sekund,
6. możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne),
7. ochrony dostępu poprzez konfigurowalny kod PIN,