OPIS PRZEDMIOTU ZAMÓWIENIA

I. Ogólny opis przedmiotu zamówienia.

Przedmiotem zamówienia jest:

1. Dostarczenie rocznej licencji uprawniającej Zamawiającego do aktualizacji wzorców zagrożeń do, eksploatowanego przez Zamawiającego, oprogramowania McAfee Complet EndPoint Protection – Busines (zwanego dalej **oprogramowaniem antywirusowym**). Zakres zamówienia dotyczącego licencji na oprogramowanie antywirusowe oraz szczegółowy opis znajdują się w pkt. II.
2. Dostarczenie rocznej licencji uprawniającej Zamawiającego do aktualizacji wzorców zagrożeń McAfee Email Protection oraz licencji na gwarancyjne wsparcie techniczne producenta do McAfee Email Gateway. McAfee Email Protection oraz McAfee Email Gateway tworzą razem, eksploatowany przez Zamawiającego, **system antyspamowy**. Zakres zamówienia dotyczącego licencji na system antyspamowy oraz szczegółowy opis znajdują się w pkt. III.

   lub

3. Zapewnienie rozwiązania równoważnego do licencji na oprogramowanie antywirusowe i system antyspamowy. Licencje na rozwiązanie równoważne obowiązujące przez okres 1 roku od dostarczenia licencji. Szczegółowy opis równoważności znajduje się w pkt IV.

II. Zakres zamówienia dotyczącego oprogramowania antywirusowego.

1. Wykonawca dostarczy Zamawiającemu licencję producenta oprogramowania antywirusowego na zapewnienie aktualizacji zagrożeń dla zasobów, podanych poniżej, objętych ochroną, tj.:
   1) 600 stacji roboczych (komputerów stacjonarnych i laptopów działających pod kontrolą systemu operacyjnego: MS Windows 8.1 Prof. i Enterprise w wersjach 32 i 64 bit oraz Windows 10 Prof. i Enterprise w wersji 64 bitowej.
   2) 34 serwery fizyczne,
   3) 71 serwerów wirtualnych,
   4) 700 skrzynek pocztowych MS Exchange,
   5) 700 użytkowników portalu wielofunkcyjnego SharePoint.

III. Zakres zamówienia dotyczącego systemu antyspamowego.

1. Wykonawca dostarczy Zamawiającemu licencję producenta na zapewnienie aktualizacji zagrożeń do oprogramowania McAfee Email Protection wykorzystywanego do ochrony zasobów:

1) 700 stacji roboczych (komputerów stacjonarnych i laptopów działających pod kontrolą systemu operacyjnego: MS Windows 8.1 Prof. i Enterprise w wersjach 32 i 64 bit oraz Windows 10 Prof. i Enterprise w wersji 64 bitowej.
2) 700 skrzynek pocztowych.

2. Wykonawca zapewni Zamawiającemu licencję na gwarancyjne wsparcie techniczne producenta do 2 urządzeń McAfee Email Gateway EG4500-C Appliance działających w klastrze. Gwarancyjne wsparcie techniczne obejmuje:

1) Zdalną pomoc techniczną w miejscu pracy 5x10 (5 dni w tygodniu pn-pt przez 10 godzin).
2) Realizacje napraw gwarancyjnych w miejscu instalacji urządzenia, w terminie 10 dni roboczych od zgłoszenia.
3) W przypadku wystąpienia awarii urządzenia skutkującej wymianą urządzenia, nowe urządzenie zostanie dostarczone Zamawiającemu w terminie 10 dni od stwierdzenia konieczności wymiany.
4) Zapewnienie ciągłego (24h na dobę, we wszystkie dni) dostępu do bazy wiedzy producenta.
5) Elektroniczne składanie zapytań.
6) Aktualizacje oprogramowania urządzeń (products update & upgrade).

IV. Opis równoważności.

Zamawiający dopuszcza możliwość dostawy rozwiązania równoważnego do opisanych w pkt. II i III.
Za rozwiązanie równoważne Zamawiający uzna rozwiązanie spełniające wymagania opisane w pkt. II (ppkt. 1) i pkt III (ppkt 1 pppkt 1-2 i ppkt 2 pppkt 1-6) oraz poniższe wymagania:

1. Dostawę oprogramowania i urządzeń o wydajności I funkcjonalności nie gorszej od posiadanych przez Zamawiającego.
2. Spełniających szczegółowe wymagania opisane w pkt V i VI OPZ.
3. Zapewnienie usługi kompletnej nieinwazyjnej deinstalacji dotychczasowego oprogramowania antywirusowego i systemu antyspamowego z całej infrastruktury informatycznej (komputerów i serwerów) Zamawiającego.
4. Zapewnienie usługi kompletnej nieinwazyjnej instalacji i konfiguracji nowego rozwiązania w infrastrukturze informatycznej Zamawiającego.
5. Zapewnienia dodatkowego wsparcia technicznego (zdalnego oraz, w razie potrzeby, bezpośredniego – realizowanego w siedzibie Zamawiającego) przez Wykonawcę przez okres miesiąca od daty wdrożenia produkcyjnego rozwiązania równoważnego.
6. Przeszkolenie do 5 pracowników Zamawiającego z zakresu obsługi, konfiguracji i administracji całości rozwiązania równoważnego.
7. Wdrożenie, szkolenie, asysta techniczna i dodatkowe wsparcie techniczne Wykonawcy – w języku polskim.

8. Usługi wdrożeniowe równoważnego oprogramowania antywirusowego i systemu antyspamowego zostaną zrealizowane w terminie do …(zgodnie z ofertą wykonawcy) dni roboczych od daty zawarcia umowy.

9. Usługi wdrożeniowe obejmują:

   a) Montaż urządzeń w serwerowni Zamawiającego.

   b) Deinstalację dotychczasowych rozwiązań (oprogramowanie antywirusowe i system antyspamowy McAfee.

   c) Instalacje, konfiguracje i uruchomienie produkcyjne oprogramowania antywirusowego i systemu, zgodnie z zaleceniami Zamawiającego.

   d) Świadczenie bezpośredniej, w siedzibie Zamawiającego, asysty technicznej przez cały okres od rozpoczęcia wdrożenia do 5 dni roboczych od uruchomienia produkcyjnego całości rozwiązania równoważnego.

   e) Szkolenia.

V. Wymagania w stosunku do wdrożenia równoważnego oprogramowania antywirusowego.

1. Moduł ochrony antywirusowej i antyspyware.

2) Moduł musi poprawnie współpracować z następującymi systemami operacyjnymi wykorzystywanymi przez Zamawiającego:

   a) Microsoft Windows 10
   b) Microsoft Windows 10 x64 Edition
   c) Microsoft Windows 8.1,
   d) Microsoft Windows 8.1 x64 Edition,
   e) Microsoft Windows Server 2008,
   f) Microsoft Windows Server 2008 R2,
   g) Microsoft Windows Server 2012,
   h) Microsoft Windows Server 2012 R2,
   i) Microsoft Windows Server 2016

3) Moduł ochrony stacji roboczych musi posiadać polskojęzyczny interfejs.

4) Moduł powinien zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hackerskich, oprogramowania typu spyware i adware, rootkit, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.

5) Ochrona antywirusowa musi być realizowana na podstawie:
   a) sygnatur,
   b) heurystyki (z możliwością jej wyłączenia),
   c) na bieżąco weryfikowanej informacji o nowych zagrożeniach w bazie producenta dostępnej przez Internet.

6) Moduł musi mieć możliwość określenia listy reguł wykluczeń dla wybranych obiektów,

rodzajów zagrożeń oraz składników ochrony.

7) Moduł musi umożliwiać skanowanie antywirusowe w chwili dostępu (real time), na żądanie i według harmonogramu z następującymi warunkami:
   a) skanowanie na żądanie i wg harmonogramu musi mieć możliwość przerwania w dowolnym momencie,
   b) skanowanie na żądanie musi mieć możliwość wstrzymania w przypadku wykrycia pracy na baterii,
   c) skanowanie na żądanie musi mieć możliwość wstrzymania w przypadku wykrycia pracy w trybie pełnoekranowym (np. prezentacja).
8) Moduł musi wykrywać zagrożenia: na dyskach, w plikach w tym archiwach plikowych, na stronach web, w przesyłkach email w tym w załącznikach, na podłączanych nośnikach przenośnych.
9) Moduł musi współpracować z Windows Action Center oraz dla Windows 8 musi współpracować z Early Launch Anti-malware (ELAM), wykorzystywanymi przez Zamawiającego.
10) Moduł musi zapewniać ochronę komunikacji przy wykorzystaniu protokołów POP3, SMTP, IMAP i NNTP w czasie rzeczywistym niezależnie od klienta pocztowego.
11) Moduł musi zapewniać ochronę komunikacji przy wykorzystaniu protokołu HTTP w czasie rzeczywistym niezależnie od przeglądarki.
12) Moduł musi zawierać programy (pluginy do przeglądarek Microsoft IE, Mozilla Firefox i Google Chrome) działające na stacjach użytkowników i ostrzegające ich o złośliwej zawartości strony internetowej wraz z możliwością aktywnego blokowania dostępu do wybranych stron internetowych, określonych centralnie przez administratora systemu. Rozwiązanie musi realizować także możliwość określenia blokowanych stron web na podstawie kategorii strony (np. pornografia, strony społecznościowe, itp.).
13) Moduł musi umożliwiać ustawienia priorytetu procesu skanowania.
14) Aktualizacja wzorców wirusów musi odbywać się co najmniej raz dziennie.
15) Moduł musi umożliwiać aktualizację wzorców wirusów z archiwum internetowego lub z centralnego punktu dystrybucji wzorców wirusów.
16) Moduł musi umożliwiać pobieranie aktualizacji za pośrednictwem serwera Proxy.
17) Po wykryciu zagrożenia musi istnieć możliwość oczyszczenia zainfekowanego pliku a jeśli nie jest to możliwe – usunięcia bądź umieszczenia go w lokalnej kwarantannie.
18) W przypadku zainstalowania na urządzeniach przenośnych musi nastąpić automatyczna zmiana punktu dystrybucji wzorców na archiwum internetowe bez konieczności ingerencji użytkownika.
19) Moduł musi umożliwiać konfigurowanie dostępności i zakresu ingerencji użytkownika w proces skanowania.
20) Moduł musi umożliwiać zabezpieczanie hasłem przed zmianą konfiguracji, deinstalacją i zatrzymaniem programu.

21) Moduł musi wymuszać odświeżanie wzorców wirusów.

22) Moduł musi mieć możliwość instalacji oprogramowania klienckiego przy pomocy systemu SCCM.

23) Uaktualnienia oprogramowania (silnik) musi być dostępne przez cały okres trwania abonamentu bazy wzorców wirusów (trwania umowy).

2. Moduł firewalla.

1) Zapora osobista musi umożliwiać:
   a) tworzenie reguł monitorowania aktywności sieciowej dla wszystkich zainstalowanych aplikacji w oparciu o charakterystyki pakietów sieciowych i podpis cyfrowy aplikacji,
   b) tworzenie nowych zestawów warunków i działań wykonywanych na pakietach sieciowych oraz strumieniach danych dla określonych protokołów, portów i adresów IP,
   c) pracę w trybie stanowym (stateful) dla aplikacji i procesów systemu operacyjnego,
   d) blokowanie określonych portów sieciowych,
   e) pracę firewalla w trybie nauki,
   f)tworzenie reguł firewalla działających w zależności od rodzaju połączenia (sieć firmowa, sieć publiczna),
   g) blokowanie połączeń do innych sieci (np. przez WiFi) w czasie, kiedy stacja jest podłączona do sieci firmowej,
   h) ciągłe aktualizowanie danych o reputacji adresów IP, do których/z których jest nawiązywane połączenie ze stacji oraz blokowanie połączeń związanych z wysokim ryzykiem. Informacja o reputacji musi być dostępna na bieżąco przez Internet z bazy danych prowadzonej przez producenta rozwiązania.

2) Moduł musi umożliwiać tworzenie list sieci zaufanych.

3) Moduł musi mieć możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.

4) Moduł musi mieć wbudowany system IDS/IPS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.

5) Moduł musi mieć możliwość wykrywania zmian w aplikacjach korzystających z sieci i informowanie o tym zdarzeniu.

6) Program musi oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.

7) Moduł musi umożliwiać tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci, w tym:
   a) musi istnieć możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci,
   b) musi być możliwość automatycznego przełączania profili, bez ingerencji użytkownika lub administratora.

8) Autoryzacja stref musi odbywać się co najmniej w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowanie sieci bezprzewodowej lub jego braku, aktywność połączenia bezprzewodowego lub jego braku, aktywność wyłącznie

jednego połączenia sieciowego lub wielu połączeń sieciowych, konkretny interfejs sieciowy w systemie.

3. Moduł ochrony serwera poczty MS Exchange

1) Musi być zgodny z MS Exchange 2013 wykorzystywanym przez Zamawiającego.
2) Musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.
3) Moduł musi zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hackerskich, oprogramowania typu spyware i adware, rootkit, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.
4) Moduł musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
5) Moduł musi umożliwiać skanowanie bezpośrednio w storach Exchange.
6) Moduł musi mieć możliwość zdefiniowania kilku wątków skanujących – aby przyśpieszyć pracę serwera.
7) Moduł musi mieć możliwość skanowania przed zapisaniem wiadomości w storze przy pomocy transport agenta.
8) W przypadku wykrycia wirusa/blokowania wiadomości musi istnieć możliwość usunięcia wiadomości/załącznika, wyleczenia, podmiany załącznika na czysty plik zawierający jedynie informację o infekcji.
9) Moduł musi umożliwiać tworzenie różnych reguł blokowania wiadomości wg zdefiniowanego nadawcy, odbiorcy, temacie, treści, nazwie załącznika i wielkości wiadomości, częstości występowania.
10) Moduł musi umożliwiać tworzenie białych i czarnych list domen/adresów IP, adresów e-mail.
11) Wbudowany w oprogramowanie mechanizm antyspamowy musi być odpowiedzialny za filtrowanie niechcianej poczty.
12) Mechanizm antyspamowy musi być wyposażony przynajmniej w filtr Bayesa, sprawdzanie list RBL oraz kontrolę reputacji poczty.
13) Moduł musi umożliwiać stworzenie kwarantanny dostępnej dla użytkownika.
14) Moduł musi umożliwiać ustawienie poziomów logowania, co najmniej (diagnostyczne, informacyjne, ostrzeżenia, błędy, krytyczne ostrzeżenia).
15) Moduł musi realizować skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
16) Moduł musi zapewnić skanowanie plików spakowanych i skompresowanych.
17) Moduł musi zapewnić skanowanie ruchu HTTP lokalnego serwera. Zainfekowany ruch musi być automatycznie blokowany a użytkownikowi wyświetlane stosowne powiadomienie.
18) Administrator musi mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.

19) Moduł musi skanować i oczyszczać w czasie rzeczywistym pocztę przychodzącą i wychodzącą obsługiwaną przy pomocy programu MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird (wersja 4.x i wyższa) i Windows Live Mail.
20) Moduł musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
21) Moduł musi zapewnić automatyczną integrację skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
22) Moduł musi mieć możliwość definiowania różnych portów dla POP3, na których ma odbywać się skanowanie.
23) Moduł musi mieć możliwość utworzenia kilku zadań skanowania (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (metody skanowania, obiekty skanowania, czynności).
24) Moduł musi zapewnić aktualizację modułu analizy heurystycznej.
25) Moduł musi mieć możliwość wyłączenia skanowania przy pomocy bazy sygnatur wirusowych (skanowanie samą heurystyką).
26) Moduł musi zapewnić używanie heurystycznych metod do wykrywania infekcji.
27) W przypadku wykrycia wirusa, moduł musi wysłać ostrzeżenie do administratora poprzez e-mail.
28) Moduł musi umożliwiać prowadzenie dziennika zdarzeń rejestrującego informacje na temat znalezionych wirusów, dokonanych aktualizacji baz wirusów i wersji oprogramowania.
29) Moduł musi mieć możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu.
30) Moduł musi mieć możliwość zabezpieczenia hasłem wyłączenia programu antywirusowego oraz jego odinstalowania.
31) Moduł musi zapewnić codzienną aktualizację wzorców wirusów z archiwum internetowego.
32) Aktualizacja mus być dostępna z: Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
33) Moduł musi umożliwiać pobierania aktualizacji za pośrednictwem serwera Proxy.

4. Moduł ochrony portalu wielofunkcyjnego MS Share Point

1) Moduł musi zapewniać poprawna współpracę z posiadanym przez Zamawiającego MS Share Point 2013.
2) Moduł musi zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hackerskich, oprogramowania typu spyware i adware, rootkit, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.

3) Moduł musi zapewnić wykrywanie zagrożeń na podstawie sygnatur i heurystyk
4) Moduł musi zapewnić skanowanie w poszukiwaniu szkodliwych obiektów i niepożądanych treści w czasie rzeczywistym, na żądanie lub zgodnie z zaplanowanym harmonogramem. Moduł musi zapewnić blokowanie plików zawierających szkodliwe obiekty lub niepożądane treści przy próbach przesłania ich na serwer.
5) Moduł musi zapewnić kontrolę linków pod kątem złośliwego oprogramowania lub phishingu.
6) Moduł musi zapewnić codzienną aktualizację wzorców wirusów z archiwum internetowego.

5. Moduł ochrony urządzeń mobilnych

Moduł do ochrony urządzeń mobilnych musi spełniać następujące wymagania i zapewnić:

1) Ochronę urządzeń pracujących pod kontrolą wykorzystywanych przez Zamawiającego systemów:
   a) Windows Phone 8 i późniejsze,
   b) Google Android 2.3 i późniejsze.
2) Ochronę plików w czasie rzeczywistym.
3) Skanowanie plików systemowych, bibliotek, plików archiwum oraz innych.
4) Skanowanie dostępnego w urządzeniu nośnika pamięci SD.
5) Ochronę proaktywną wykrywającą nieznane zagrożenia.
6) Określenie poziomu głębokości skanowania plików archiwum.
7) Określenie domyślnej akcji podejmowanej w przypadku wykrycia zagrożenia: przeniesienia do kwarantanny, usunięcia lub zignorowania.
8) W przypadku wykrycia zagrożenia użytkownik musi otrzymać odpowiednie powiadomienie.
9) Włączenie blokady urządzenia mobilnego na hasło alfanumeryczne o zadanej złożoności: np. minimum 8 znaków składających się z liter małych i dużych, oraz cyfr i znaków specjalnych.
10) Ustalenie czasu po którym włącza się blokada urządzenia (np. blokada ekranu po 5 minutach nieaktywności użytkownika).
11) Pamięć historii haseł blokady urządzenia, wykluczająca możliwość użycia co najmniej 5 ostatnich haseł.
12) Instalację klienta zarządzającego z poziomu Windows Storę lub Google Android Market.
13) Możliwość oddzielenia danych korporacyjnych od danych prywatnych, w tym kalendarzy, możliwość ustalenia aplikacji mającej dostęp do poczty korporacyjnej oraz aplikacji które mogą otwierać załączniki.
14) Możliwość wykrywania ingerencji w oryginalne oprogramowanie urządzenia.

6. Centralna konsola zarządzająca

1) Moduł musi zapewnić centralną instalację programów służących do ochrony stacji roboczych Windows.
2) Moduł musi zapewnić centralne zarządzanie wszystkimi programami służącymi do ochrony: stacji roboczych, serwerów plików, serwerów pocztowych, serwerów portalu wielofunkcyjnego, aplikacji mobilnych.
3) Moduł musi posiadać centralną bazę przechowującą informacje o konfiguracji stacji i urządzeń końcowych.
4) Moduł musi posiadać centralną bazę przechowującą informacje o zdarzeniach i wykrytych zagrożeniach.
5) Centralna konsola zarządzająca musi umożliwić zdalną instalację produktów na komputerach z domeny Microsoft Active Directory objętych ochroną, bez konieczności stosowania dodatkowych narzędzi i oprogramowania, z możliwością zaplanowania z wyprzedzeniem momentu wykonania instalacji dla poszczególnych komputerów i grup komputerów.
6) Oferowane rozwiązania musi umożliwiać selektywne wskazanie, który z produktów ochronnych wchodzących w skład systemu zostanie wdrożony na którym z komputerów - nie jest dopuszczalne wdrożenie pakietu w postaci jednej paczki instalacyjnej obejmującej kilka produktów na raz.
7) Moduł musi mieć możliwość definiowanie komputerów, które mają być objęte wdrożeniem poszczególnych produktów, musi być możliwe na bazie zdefiniowanych grup maszyn oraz na bazie dynamicznie przydzielanych znaczników, niezależnie od podziału na grupy maszyn, uzależnionych od parametrów komputera - co najmniej takich jak: rodzaj CPU, ilość RAM, wielkość dysku, rodzaj systemu operacyjnego, ilość dostępnego miejsca na dysku.
8) Moduł nie musi zawierać dodatkowego agenta do centralnej instalacji i zarządzania.
9) Moduł musi szyfrować komunikację między serwerem a klientami.
10) Moduł musi zapewnić centralną konfiguracje i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
11) Moduł musi być wyposażony w kreator konfiguracji zapory osobistej stacji klienckich pracujących w sieci, umożliwiający podgląd i utworzenie globalnych reguł w oparciu o reguły odczytane ze wszystkich lub z wybranych komputerów lub ich grup.
12) Moduł musi mieć możliwość uruchomienia centralnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej.
13) Moduł musi mieć możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie i skanerów rezydentnych).

14) Moduł musi mieć możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego, aktualnie zalogowanego uzytkownika oraz domeny, do której dana stacja robocza należy.

15) Moduł musi umożliwiać centralną aktualizację stacji roboczych z serwera w sieci lokalnej lub z Internetu.

16) Moduł musi mieć możliwość utworzenia centralnego punktu dystrybucji wzorców wirusów.

17) Moduł musi mieć możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych.

18) Moduł musi mieć możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów.

19) Moduł musi mieć możliwość importowania konfiguracji programu z wybranej stacji roboczej a następnie przesłanie (skopiowanie) jej na inną stację lub grupę stacji roboczych w sieci.

20) Moduł musi mieć możliwość zmiany konfiguracji na stacjach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko, jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne).

21) Moduł musi mieć możliwość uruchomienia serwera centralnej administracji i konsoli zarządzającej na wykorzystywanych przez Zamawiającego stacjach Windows 10 ,8, 7, Windows Server 2016,2012 R2, 2012, 2008 R2, 2008.

22) Centralna konsola zarządzająca musi posiadać możliwość powiadamiania o wszystkich zdarzeniach za pomocą poczty elektronicznej, wiadomości SNMP i syslog lub wywołania komendy/skryptu.

23) Centralna konsola zarządzająca musi mieć możliwość integracji z Active Directory zarówno w rozumieniu powielenia struktury komputerów jak i autentykacji administratorów i dynamicznego przypisywania uprawnień w serwerze zarządzającym w zależności od przynależności do odpowiedniej grupy w Active Directory.

24) Centralna konsola zarządzająca musi umożliwiać zdefiniowanie wielu kont administratorów i przydzielenie im szczegółowych ról umożliwiających co najmniej: ograniczenie dostępu do wskazanych grup maszyn, ograniczenie administracji do poszczególnych produktów i ich specyficznych funkcji.

7. Wymagania szczegółowe dla usług wdrożenia równoważnego oprogramowania antywirusowego.

Wykonawca zobowiązuje się do realizacji usług wdrożeniowych:

1) Instalacja, konfiguracja i uruchomienie centralnej konsoli zarządzającej.

2) Instalacja, konfiguracja i uruchomienie oprogramowania na serwerach poczty MS Exchange.

3) Instalacja, konfiguracja i uruchomienie oprogramowania na portalu wielofunkcyjnym serwerów MS Share Point.
4) Instalacja, konfiguracja i uruchomienie oprogramowania na wybranych 600 stacjach roboczych z wykorzystaniem centralnej konsoli zarządzającej.
5) Instalacja, konfiguracja i uruchomienie oprogramowania na 34 serwerach fizycznych i 71 wirtualnych pracujących pod kontrolą systemu MS Windows 2012r2 lub 2016 z wykorzystaniem centralnej konsoli zarządzającej.
6) Przeprowadzenie szkoleń administratorów Zamawiającego:
   a) Obejmujące zakresem instalację, deinstalację konfigurację.
   b) Wykonawca zapewni min. 2 szkolenia w wymiarze min 4 godzin każde dla grupy nie większej niż 5 osób.
   c) Szkolenia będą zrealizowane w siedzibie Zamawiającego.
   d) Szkolenia będą odbywały się w terminie uzgodnionym z Zamawiającym. Pierwsze szkolenie przeprowadzone będzie nie później niż 15 dni od rozpoczęcia instalacji oprogramowania.

8. Wymagania szczegółowe dla usług wsparcia równoważnego oprogramowania antywirusowego.

Wykonawca zobowiązuje się do zapewnienia Zamawiającemu usług wsparcia równoważnego przez okres 1 roku od daty rozpoczęcia instalacji oprogramowania w minimalnym zakresie:

1) Zapewnienie aktualnych i historycznych wzorców ataków.
2) Udostępnienie uaktualnień i poprawek do zaoferowanego systemu.
3) Udostępnienie bazy wiedzy: dokumentacji technicznej, listy najczęściej zadawanych pytań i forum użytkowników.
4) Konsultacje w zakresie konfiguracji, eksploatacji i instalacji w formie serwisu telefonicznego dostępnego w dni robocze, w godzinach 9:00-17:00.
5) Usługi serwisowe w zakresie usuwanie awarii, które będą świadczone na następujących zasadach:
   - Przyjmowanie zgłoszeń poprzez serwis telefoniczny dostępny w dni robocze, w godzinach 9:00-17:00 lub poprzez pocztę elektroniczną wysłaną na adres ..... .
   - Wykonawca przystąpi do realizacji zgłoszenia obsługi serwisowej i poinformuje o tym fakcie Zamawiającego w terminie 2 dni roboczych od otrzymania zgłoszenia.
   - Zrealizowanie zgłoszenia obsługi serwisowej nastąpi w terminie 10 dni roboczych od dnia zgłoszenia.

VI. Wymagania w stosunku do wdrożenia równoważnego systemu antyspamowego.

1. Wymagania ogólne

1) System musi obsługiwać nie mniej niż 700 użytkowników.
2) System musi umożliwiać obsługę ruchu email na poziomie min. 35 tysięcy przesyłek dziennie.
3) W ramach dostawy systemu ochrony należy zapewnić licencje na oprogramowanie ochronne.

2. Parametry techniczne

1) Obudowa typu 1U.
2) Minimalna liczba interfejsów sieciowych urządzenia to co najmniej 2 interfejsy 100/1000 Mbps.
3) Urządzenie ma być wyposażone w redundantną macierz dysków typu RAID.
4) Ilość przestrzeni dyskowej przeznaczonej na kwarantannę to minimum 50GB.
5) Minimalna wielkość cache dla logów to 20 Gb.
6) System musi umożliwiać wdrożenie w trybie proxy aplikacyjnego (mail relay), routera (transparent router) oraz transparent bridge
7) W każdym z trybów pracy powinna być zachowana taka sama funkcjonalność ochrony poczty przed spam i kodem złośliwym
8) Rozwiązanie musi posiadać wbudowane mechanizmy budowy klastra wysokiej dostępności (HA) oraz współdzielącego ruch dla rozłożenia obciążenia między urządzenia wchodzące w skład klastra.
9) Oferowane rozwiązanie musi spełniać wymogi niezbędne do oznaczenia znakiem CE.

3. Wymagania dotyczące implementacji sieciowej

1) Rozwiązanie ma działać w warstwie sieciowej (gateway poczty elektronicznej) i musi obsługiwać co najmniej protokoły SMTP i POP3, przy czym musi być możliwe określenie portów na jakich działają te protokoły.
2) System musi umożliwiać wysyłanie wiadomości SNMP, syslog oraz powiadomień w formie poczty elektronicznej dla zdefiniowanych zdarzeń.
3) System musi posiadać możliwość monitorowania z zewnątrz za pomocą SNMP.
4) System musi posiadać wbudowane wydajne mechanizmy ograniczania skutków ataków typu Denial of Service (DoS) z wykorzystaniem poczty elektronicznej co najmniej takie, jak:
    a. określenie maksymalnego czasu pomiędzy komendami SMTP,

b. określenie minimalnej przepustowości przesyłania danych,
c. określenie maksymalnej liczby tzw. trywialnych komend SMTP,
d. określenie maksymalnej ilości odbiorców wiadomości,
e. określenie maksymalnej długości połączenia SMTP,
f. określenie maksymalnej długości części domenowej adresu,
g. stosowanie technik zapobiegających przed atakami Directory Harvest, gdzie można zdefiniować ile procentowo odbiorców musi być niepoprawnych w stosunku do wszystkich by zablokować połączenie od nadawcy.

5) System musi posiadać mechanizmy routingu poczty elektronicznej – kierowania jej zależnie od domeny do różnych hostów (MTA, serwer pocztowy)

6) System ma zapewniać ochronę anti-relay.

7) System musi mieć możliwość ochrony przed spamem przez użycie graylistingu.

4. Wymagania dotyczące ochrony anty-spamowej (AS)

1) System ma:

a. zapewniać ochronę zarówno poczty przychodzącej jak i wychodzącej,
b. zapobiegać próbom spoofingu, phisingu i spyware,
c. zabezpieczać przed atakami typu DoS (Denial of Service),
d. zabezpieczać pocztę wychodzącą, w skład której wchodzi ochrona antywirusowa, kontrola ilości wysłanych wiadomości przez użytkownika,
e. zapewniać ochronę przed atakami typu DHA (Directory Harvest Attack).

2) Skaner AS musi działać w oparciu o system oceny prawdopodobieństwa wystąpienia spamu bazujący na regułach aktualizowanych przez producenta.

3) Aktualizacja reguł musi odbywać się na bieżąco kilka razy na godziną, a co najmniej raz dziennie.

4) Skaner AS musi współpracować z serwerami AD i LDAP pozwalając na stworzenie dokładnej polityki skanowania zależnie od adresu email, grupy użytkowników w AD/LDAP, domeny pocztowej, zakresu adresów IP.

5) System AS musi obsługiwać białe i czarne listy (blacklist i whitelist) definiowane przez administratora oraz samodzielnie przez końcowych użytkowników (odbiorców poczty).

6) Możliwość ustawiania progów na podstawie punktacji przypisanej przez algorytmy modułu antyspamowego dla wiadomości przychodzących, wg której wiadomości mogą być blokowane, przesyłane do kwarantanny lub oznaczane jako spam.

7) System AS musi obsługiwać technologie graylist, SPF oraz Sender ID.

8) System powinien umożliwiać rozpoznawanie URL'i w treści wiadomości i filtrować wiadomość i URL'ami o złej reputacji. Kontrola reputacji URL powinna być badana w momencie dostarczania wiadomości oraz w momencie kliknięcia URL'a przez użytkownika w kliencie pocztowym w czasie rzeczywistym.

9) System AS musi posiadać filtr reputacyjny badający domenę i adres IP, z których nadana została wiadomość oraz zawartość przesyłaną w email.

10) Reputacja powinna być określona dynamicznie, na bieżąco przez zapytania do serwisu reputacyjnego prowadzonego przez producenta rozwiązania.

11) Musi być możliwe zdefiniowanie różnych akcji podejmowanych po wykryciu spamu zależnie od określonego przez system prawdopodobieństwa wykrycia spam (spam score):

   a. zablokowanie i skasowanie wiadomości z powiadomieniem do końcowego użytkownika, a także bez takiego powiadomienia (zależnie od przyjętej polityki),
   b. przekazanie wiadomości do kwarantanny,
   c. przesłanie wiadomości do odbiorcy z oznakowaniem jej jako spam w tytule wiadomości
   d. dodanie do nagłówka wiadomości informacji o punktacji (*spam score)*,
   e. dodanie do nagłówka wiadomości informacji, które reguły ant-spamowe spowodowały wykrycie spam.

5. Wymagania dotyczące tworzenia polityki działania Gateway'ów

1) Każde z urządzeń musi współpracować z serwerami Active Directory i LDAP pozwalając na autentykację odbiorcy poczty i stworzenie dokładnej polityki skanowania poczty uzależnionej od grup użytkowników lub poszczególnych użytkowników pochodzących z AD i LDAP.

   a. musi być zapewnione wsparcie co najmniej dla następujących rodzajów LDAP: AD, MS Exchange, Generic LDAP Server v3,
   b. musi istnieć możliwość odpytania serwera AD/LDAP na bieżąco lub zdefiniowanie okresowej synchronizacji danych z AD/LDAP,

2) Integracja z AD/LDAP musi umożliwiać także realizację:

   a. maskowania realnych adresów email w zależności od wpisu w AD/LDAP,
   b. decyzje o sposobie (ścieżce – route) dostarczenia poczty,

3) System musi pozwalać na stworzenie dokładnej polityki skanowania zależnie od danej domeny pocztowej, adresu źródłowego/docelowego, użytkownika lub grupy użytkowników, numeru VLAN (w trybie transparent bridge):

   a. musi być możliwe definiowanie równocześnie wielu polityk, których zastosowanie zależy od kolejności na liście polityk i w/w kryteriów,
   b. musi być możliwe tworzenie osobnych polityk dla wiadomości wychodzących i dla przychodzących.

4) Sposób konfigurowania polityki działania Systemu musi umożliwiać definiowanie kilku jednoczesnych reakcji na wykryte zdarzenie – na przykład:

   a. zablokowanie wiadomości i wysłanie niezależnego powiadomienia o tym zdarzeniu pod wskazany adres email
   b. przesłanie poczty do odbiorcy, a dodatkowo przesłanie jej kopii pod wskazany adres
   c. zablokowanie wiadomości i skierowanie jej do kwarantanny

5) System musi usuwać z nagłówków wiadomości email informacje dotyczące wewnętrznej infrastruktury Zamawiającego, mogących posłużyć do jej rozpoznania przez osoby nieupoważnione

6) Rozwiązanie musi obsługiwać aliasy pocztowe oraz umożliwiać automatyczne, zależne od przyjętej konfiguracji, dodawanie do poczty wychodzącej zdefiniowanego zapisu tzw. Disclaimer.

7) Rozwiązanie, w ramach poszczególnych polityk, musi umożliwiać ograniczanie :

   a. maksymalnej wielkości przesyłki pocztowej,
   b. maksymalnej wielkości załącznika do email,
   c. maksymalnej ilości załączników do email.

8) Rozwiązanie musi umożliwiać filtrowanie poczty pod kątem przesyłanych obrazów/zdjęć zawierających treści erotyczne i pornograficzne:

   a. filtr musi analizować obrazy/zdjęcia pod kątem ich zawartości w czasie rzeczywistym,
   b. filtracja nie może wymagać wcześniejszego zarejestrowania blokowanych zdjęć / obrazów lub jakiegokolwiek innego uprzedniego określania, które zdjęcia/obrazy mają podlegać filtracji

9) System musi umożliwiać filtrację poczty na podstawie jej zawartości:

   a. rozwiązanie musi przeprowadzać filtrowanie treści według zdefiniowanych reguł, w co najmniej 100 rodzajach/formatach przesyłanych plików,
   b. musi być możliwe filtrowanie wiadomości z załączonymi plikami na podstawie ich nazw,
   c. musi być możliwe filtrowanie wiadomości na podstawie ich wielkości,
   d. musi być możliwe blokowanie wiadomości zawierających załączniki zaszyfrowane lub spakowane z hasłem.

6. Wymagania dotyczące wykrywania kodu złośliwego (AM)

1) System musi być wyposażony w skaner anti-malware (AM).

2) Skaner AM musi wykorzystywać dzienne, automatyczne aktualizacje baz sygnatur antywirusowych:

   a. musi istnieć możliwość określenia częstotliwości i harmonogramu aktualizacji silnika AM i baz sygnatur.

3) Skaner AM musi posiadać mechanizm wykrywający nowe zagrożenia w technologii „in the cloud” za pomocą serwisów reputacyjnych posiadanych przez producenta rozwiązania:

   a. W razie wykrycia podejrzanego kodu/pliku i braku definicji w lokalnym pliku sygnatur anty-wirusowych, skaner AM musi mieć możliwość wysłania zapytania do centralnej bazy prowadzonej przez producenta rozwiązania o to czy dany plik/kod jest już znany i zakwalifikowany jako zagrożenie,
   b. Zależnie od wyniku zapytania, skaner AM musi mieć możliwość podjęcia takiej samej reakcji jak w przypadku wykrycia zagrożenia na podstawie lokalnego pliku sygnatur.

4) Skaner AM musi wykrywać i blokować oprogramowanie szpiegujące oraz wykrywać próby ataków typu PHISHING.

5) Skaner AM musi wykrywać wykorzystanie mechanizmów kompresji (archiwizery, packery) używanych przez szkodliwe oprogramowanie i musi umożliwiać automatyczne skasowanie plików przygotowanych z ich użyciem.

6) Skaner AM musi skanować media strumieniowe oraz umożliwiać wyłączanie ze skanowania określonych w polityce typów tych mediów.

7) Skaner AM musi umożliwiać blokowanie skryptów, apletów Java oraz ActiveX.

8) Skaner AM musi mieć możliwość stosowania konfiguracji, w której wirusy konkretnego typu (np. Mass Mailery) są zawsze usuwane przez Gateway pocztowy bez powiadamiania użytkownika, a w razie wykrycia kodu zagrożeń innego typu logowanie go standardowo.

Oprócz skanera anti-malware (AM) pochodzącego od tego samego producenta, co całe oferowane rozwiązanie powinien być dostępny inny silnik anti-malware innego producenta. Silnik ten powinien być dostarczany w ramach głównej licencji – bez dodatkowych kosztów.

7. Wymagania dotyczące zarządzania oferowanym oprogramowaniem

1) Interfejs zarządzający dostępny będzie na każdym urządzeniu osobno przez przeglądarkę internetową i połączenie https bez użycia maszyny wirtualnej Java:
   a. GUI interfejsu zarządzania musi być wyposażone w konfigurowany pulpit (dashboard), na którym znajduje się podsumowanie najważniejszych parametrów Systemu i wyników ochrony poczty,
   b. musi istnieć możliwość zdefiniowania wielu kont administratorów i przypisania im uprawnień do wykonywania tylko pewnych czynności administracyjnych (co najmniej ograniczenie dostępu tylko do konfiguracji polityk bez możliwości zmian konfiguracji sieciowej, ograniczenie dostępu tylko do modułu raportowania, ograniczenie dostępu do konfiguracji szyfrowania poczty),
   c. konta administratorów można tworzyć lokalnie w systemie oraz korzystać z zewnętrznych usług katalogowych dostępnych przez protokoły Radius i Kerberos.
2) System musi umożliwiać centralne zarządzanie wieloma urządzeniami działającymi w klastrze jak i niezależnie bez konieczności zakupu dodatkowych licencji lub oprogramowania.

3) System musi posiadać wbudowane raportowanie, bez konieczności stosowania dodatkowego oprogramowania i zewnętrznych serwerów:
   a. raporty powinny być tworzone na podstawie predefiniowanych, gotowych szablonów,
   b. musi być możliwe także tworzenie własnych raportów,
   c. raporty mają być generowane na żądanie i okresowo, według zdefiniowanego harmonogramu,
   d. musi być możliwe zapisanie Raportu, co najmniej w formacie PDF, HTML, TXT,
   e. musi być możliwe automatyczne wysłanie raportu mailem pod wskazany adres.
4) Interfejs zarządzający musi umożliwiać wizualizację przebiegu transakcji SMTP i przejścia wiadomości przez poszczególne filtry ochronne Gateway'a.

5) Interfejs zarządzający musi umożliwiać administratorowi zarządzanie wiadomościami przechowywanymi w lokalnej kwarantannie.

8. Wymagania szczegółowe dla usług wdrożenia równoważnego systemu antyspamowego.

Wykonawca zobowiązuje się do realizacji usług wdrożeniowych:

1) Montaż urządzeń w serwerowni Zamawiającego, Instalacja, konfiguracja i uruchomienie systemu zgodnie z sugestiami Zamawiającego.

2) Przeprowadzenie szkoleń administratorów Zamawiającego:

   a. Obejmujące zakresem instalację, deinstalację konfigurację.
   b. Wykonawca zapewni min. 2 szkolenia w wymiarze min 4 godzin każde dla grupy nie większej niż 5 osób.
   c. Szkolenia będą zrealizowane w siedzibie Zamawiającego.
   d. Szkolenia będą odbywały się w terminie uzgodnionym z Zamawiającym. Pierwsze szkolenie przeprowadzone będzie nie później niż 5 dni roboczych od rozpoczęcia instalacji oprogramowania.

9. Wymagania dla usług wsparcia technicznego

Wymagania szczegółowe dla usług wsparcia technicznego do równoważnego systemu antyspamowego.

Wykonawca zobowiązuje się do zapewnienia Zamawiającemu usług wsparcia przez okres 1 roku od daty rozpoczęcia instalacji systemu. Usługi obejmują:

1) Udostępnienie uaktualnień i poprawek do zaoferowanego systemu,
2) Udostępnienie bazy wiedzy: dokumentacji technicznej, listy najczęściej zadawanych pytań i forum użytkowników
3) Konsultacje w zakresie konfiguracji, eksploatacji i instalacji w formie serwisu telefonicznego dostępnego w dni robocze, w godzinach 9:00-17:00,
4) Usługi serwisowe w zakresie usuwanie awarii.
5) Usługi serwisowe będą świadczone na następujących zasadach:

   a. przyjmowanie zgłoszeń poprzez serwis telefoniczny dostępny w dni robocze, w godzinach 9:00-17:00; lub poprzez pocztę elektroniczną wysłaną na adres .....
   b. Wykonawca przystąpi do realizacji zgłoszenia obsługi serwisowej i poinformuje o tym fakcie Zamawiającego w terminie 2 dni roboczych od otrzymania zgłoszenia.
   c. zrealizowanie zgłoszenia obsługi serwisowej nastąpi w terminie 10 dni od dnia zgłoszenia.