**OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem zamówienia jest i wdrożenie systemu obejmującego funkcjonalność wielopoziomowej ochrony poczty elektronicznej. W skład Systemy wchodzi: Moduł ochrony poczty e-mail (Antyspam) – 2 szt. (klaster Active/Pasive) wraz z modułem zaawansowanej ochrony przeciwko zagrożeniom klasy Sandbox (Antymalware) – 2 szt. (klaster wysokiej dostępności HA) wraz z wdrożeniem i wsparciem producenta, wsparciem technicznym oraz szkoleniem dla administratorów.

**1. STOSOWANE DEFINICJE**

1) **Moduł** – Oprogramowanie i sprzęt fizyczny, serwery i usługi pochodzące od jednego Producenta, realizujący wymagane funkcjonalności i będący częścią Systemu
2) **Oprogramowanie** – wszystkie Moduły, programy komputerowe, aplikacje, obrazy maszyn wirtualnych, serwery fizyczne, oraz wszelkie pozostałe oprogramowanie, w tym oprogramowanie instalowane na serwerach oraz całość usług, umożliwiające realizację funkcjonalności Systemu zgodnie z umową oraz OPZ;
3) **System** – całość oferowanego rozwiązania, składającego się z wymaganych Modułów obejmującego funkcjonalność ochrony poczty elektronicznej przed zagrożeniami zawierająca wszystkie niezbędne elementy w tym: wszystkie licencje, Oprogramowanie, serwery fizyczne, umożliwiające realizację funkcjonalności Systemu zgodnie z OPZ.
4) **Producent** – osoba fizyczna lub prawna oferująca Oprogramowanie oraz serwery pod własną nazwą lub znakiem towarowym.
5) **Dni Robocze** - dni pracy, od poniedziałku do piątku, z wyłączeniem sobót i dni ustawowo wolnych od pracy.
6) **Zgłoszenie Serwisowe** – zgłoszenie Awarii Systemu przekazane poprzez zapewnione przez Wykonawcę oprogramowanie umożliwiające zdalne zgłaszanie i monitorowanie statusu zgłoszenia Awarii, przekazane przez osobę upoważnioną ze strony Odbiorcy. Zgłoszenie Serwisowe staje się skuteczne (zostaje dokonane) z chwilą w prowadzenia Zgłoszenia Serwisowego do oprogramowania umożliwiającego zdalne zgłaszanie i monitorowanie statusu zgłoszenia Awarii.
7) **Czas Reakcji –** czas liczony od momentu Zgłoszenia Serwisowego do chwili poinformowania Zamawiającego o podjęciu działań zmierzających do ustalenia przyczyn i dokonania Naprawy.
8) **Czas Naprawy** – czas liczony od momentu przekazania Zgłoszenia Serwisowego przez Zamawiającego do chwili dokonania Naprawy; do czasu Naprawy wliczany jest Czas Reakcji;
9) **Naprawa** – trwałe usunięcie awarii poprzez usunięcie przyczyny powstania awarii skutkujące przywróceniem pełnej sprawności Systemu po wystąpieniu awarii, w tym również zakończenie innych działań naprawczych.
10) **Awaria** – niesprawność Systemu uniemożliwiająca niezakłócone korzystanie ze wszystkich funkcjonalności Systemu. Za Awarię będzie uznawane również uszkodzenie/usunięcie danych, jeżeli zostało spowodowane okolicznościami, o których mowa w zdaniu pierwszym

lub w związku z Naprawą Awarii. Awarie Systemu mogą mieć charakter Awarii Krytycznej albo Awarii Niekrytycznej.

**2. WYMAGANIA DOTYCZĄCE OFEROWANEGO ROZWIĄZANIA:**

1) Oferowany System składać się musi z minimum dwóch modułów (Antyspam i Antymalware) i będzie pochodził tylko z oficjalnych kanałów dystrybucyjnych Producentów Modułów na terenie Unii Europejskiej.
2) Każdy moduł stanowiący element Systemu musi stanowić jednolite środowisko programowe, tj. współpracować ze sobą bez konieczności stosowania dodatkowych elementów nie będących standardową częścią oferowanego Modułu
3) Oferowane rozwiązanie ma stanowić jednolity i kompleksowy System składający się z wymaganych Modułów. Skalowalny i elastyczny w kontekście potencjalnej rozbudowy.
4) Wymaganiem Zamawiającego jest, aby każdy Moduł posiadał tylko jedną konsolę zarządzającą.
5) Oferowane rozwiązanie nie może być zabronione do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).
6) Oferowane rozwiązanie nie może być czasowo wstrzymane do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).
7) Zamawiający wymaga, aby wszystkie elementy i Moduły dostarczanego Systemu były w najnowszej wersji (tzn. najnowszej udostępnionej przez Producenta rozwiązania) na dzień składania ofert.
8) Żaden z modułów i elementów oferowanego Systemu na dzień składania ofert oraz przez minimum 36 miesięcy od dnia podpisania umowy nie może być przeznaczony przez producenta do wycofania z produkcji lub sprzedaży.

**3. Wymagania ogólne:**

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową, antyspyware'ową, ochronę przed próbami oszustw i wyłudzeń (phising), złośliwym oprogramowaniem (malware) bez limitu licencyjnego na ilość chronionych kont użytkowników. System musi być dostarczony jako moduły:

- (Antyspam) dwa dedykowane urządzenia tworzące klaster Active/Pasive
- (Antymalware) zaawansowana ochrona przeciwko zagrożeniom klasy Sandbox, dwa dedykowane urządzenia tworzące klaster wysokiej dostępności.

a. Moduł Sandbox musi mieć możliwość pełnej integracji z dostarczanym modułem ochrony poczty e-mail oraz współpracy z systemami zabezpieczeń NGFW (Next Generation Firewall) lub SWG (Security Web Gateway), oraz w oparciu o interfejsy programistyczne API.

Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji

programowej Wykonawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń i tradycyjne bazy sygnatur. Dostarczone rozwiązanie chroniące pocztę musi mieć możliwość pracy w trybie Gateway.

**4. Parametry fizyczne modułu ochrony poczty (Antyspam):**

1) System musi być wyposażony w minimum 3 porty Gigabit Ethernet RJ-45.
2) System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1 TB z zabezpieczaniem typu RAID 1 (Mirror).
3) System musi posiadać wbudowany port konsoli szeregowej.
4) Redundantne zasilanie z sieci 230V/50Hz.

**5. Parametry fizyczne modułu sandbox (Antymalware):**

1) System musi być wyposażony:
   a. Minimum 3 interfejsy Gigabit Ethernet RJ-45,
   b. 2 interfejsy SFP+ 10 Gbps,
   c. powierzchnie dyskową - minimum 960GB w RAID1 (Mirror).
2) System Sandbox musi być dostarczony w konfiguracji HA (High Availability) z podziałem obciążenia.
3) Elementy systemu o maksymalnej wysokości 1U z możliwością montażu w standardowej szafie teletechnicznej 19 cali.

**6. Funkcje modułu ochrony poczty (Antyspam):**

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1) Wsparcie dla co najmniej 10 domen pocztowych.
2) System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 100 tys. wiadomości/godzinę.
3) Moduł AntySpam musi realizować funkcje ochrony przed spamem i zagrożeniami bezpieczeństwa w ruchu SMTP.
4) Moduł AntySpam musi umożliwiać filtrowanie poczty zarówno przychodzącej, wychodzącej jak i komunikacji wewnętrznej miedzy różnymi domenami, dlatego musi być możliwość definiowania osobnych zestawów polityk dla każdego z kierunków przesyłania wiadomości.
5) Moduł AntySpam musi realizować następujące funkcje bezpieczeństwa poczty elektronicznej:
   a. kontrola protokołu SMTP z uwzględnieniem jego szyfrowanych wersji SSL i TLS,
   b. ochrona przed spamem,
   c. ochrona przed szkodliwą zawartością (wirusy,, itp.),
   d. ochrona przed niebezpiecznymi odnośnikami URL w treści wiadomości,
6) Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
7) Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.

8) Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
9) W ramach ochrony przed atakami Directory Harvest Moduł musi umożliwiać monitorowanie i ograniczanie ilości połączeń z jednego adresu IP w określonym przedziale czasu. Musi istnieć możliwość zdefiniowania przedziału czasu od 1 minuty do 1 godziny oraz ograniczenia maksymalnej ilości połączeń i wiadomości z jednego adresu IP.
10) Dodatkowo musi istnieć możliwość tymczasowego zablokowania na zdefiniowany czas przyjmowania wiadomości z adresów IP dla których odnotowano wiadomości zawierające określoną liczbę niewłaściwych adresatów z chronionej domeny.
11) Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
12) Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
13) Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
14) Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
15) Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
16) Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora Systemu.
17) Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
18) Ochrona przed wyciekiem informacji poufnej.
19) Skanowanie załączników zaszyfrowanych bez konieczności ich odszyfrowywania .
20) Moduł AntySpam musi wspierać mechanizm DKIM (DomainKeys Identified Mail) zarówno w zakresie weryfikacji sygnatury (ang. DKIM Verification) w wiadomościach odbieranych jak i wyliczania oraz umieszczania sygnatury w wiadomościach wysyłanych (ang. DKIM Signing). Moduł musi obsługiwać klucze DKIM o długości przynajmniej 2048 bity.
21) Weryfikacja sygnatury DKIM w wiadomościach odbieranych przez bramkę Modułu musi być włączana osobno dla każdego z trzech kierunków przesyłania wiadomości:
    a. Wiadomości przychodzące.
    b. Wiadomości wychodzące.
    c. Wiadomości wewnętrzne (dla różnych domen).
22) Mechanizm wyliczania i umieszczania sygnatury w wiadomościach wysyłanych przez bramkę musi umożliwiać zarządzanie zarówno kluczami kryptograficznymi jak i regułami ich użycia. Moduł musi wspierać minimum następujące funkcje podpisywania wiadomości kluczem DKIM:
    a. Algorytmy podpisywania RSA-SHA-1 lub RSA-SHA-256,
    b. Możliwość podpisywania następujących nagłówków wiadomości: From, Reply-To, Subject, Date, To, Cc.
    c. Możliwość podpisywania własnych nagłówków wiadomości.
    d. Możliwość podpisywania treści wiadomości (ang. Body) bez limitu rozmiaru wiadomości albo z ustaleniem jaki rozmiar wiadomości zostanie podpisany.

23) Moduł AntySpam musi wspierać mechanizm DMARC (Domain-based Message Authentication, Reporting and Conformance) z możliwością aktywacji dla każdego z trzech kierunków przesyłania wiadomości osobno:
    a. Wiadomości przychodzące.
    b. Wiadomości wychodzące.
    c. Wiadomości wewnętrzne (dla różnych domen).
24) Moduł AntySpam musi zawierać dedykowane mechanizmy pozwalające wykrywać i zapobiegać podszywaniu się pod nadawcę (ang. spoofing). W tym celu Moduł musi weryfikować nadawcę wiadomości poprzez co najmniej analizę elementów wiadomości takich jak nagłówki i nadawca na kopercie wiadomości, uwzględnienie wyników działania mechanizmów weryfikacji SPF, DKIM oraz SIDV (Sender ID Validation).
25) Moduł AntySpam bezpieczeństwa poczty musi oferować ochronę Anty-Spam opierając się o zbiór technologii automatycznie i regularnie aktualizowanych przez producenta. Zakres tych metod musi co najmniej obejmować:
    - reguły oparte o sygnatury spamu,
    - reguły leksykograficzne,
    - reguły heurystyczne.
26) Moduł AntySpam musi posiadać wbudowany mechanizm wykrywania wiadomości komercyjnych typu „Newsletter” i umożliwiać traktowanie tych wiadomości w zależności od ustalonej przez administratora Systemu polityki.
27) Moduł AntySpam musi zapewnić analizę załączników wiadomości w celu wykrycia ich rzeczywistego typu lub rozszerzenia.
28) Rozpoznanie typu pliku musi odbywać się w oparciu o dostarczoną przez producenta Systemu i automatycznie aktualizowaną bazę.
29) Moduł AntySpam musi zapewnić analizę odnośników zawartych w treści oraz załącznikach wiadomości w celu zweryfikowania kategorii stron internetowych do których prowadzą.
30) Moduł AnySpam musi oferować wbudowany moduł kwarantanny.
31) Moduł AntySpam musi umożliwiać zarządzanie kolejkami (folderami kwarantanny) do przechowywania blokowanych wiadomości w zakresie zarządzania predefiniowanymi oraz tworzenia nowych. Wiadomości kierowane do określonych kolejek muszą być przechowywane w ramach bramy lub poza nią na zasobie dostępnym przez NFS.
32) Moduł Antyspam musi zapewniać poniższe funkcje i metody filtrowania:
    a. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
    b. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
    c. Szczegółowa kontrola nagłówka wiadomości.
    d. Analiza Heurystyczna.
    e. Współpraca z zewnętrznymi serwerami RBL, SURBL.
    f. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen, lub poprzez

techniki wykrywania spamu w treści wiadomości takie jak uczenie AI na bazie wzorców lub logiki rozmytej.

g. Kontrola w oparciu o SPF, DKIM oraz DMARC.
h. Filtrowanie treści wiadomości i załączników.
i. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
j. Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antyspamowej.
k. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
l. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.

33) Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Muszą one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
34) Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
35) Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
36) Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
37) Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
38) Weryfikacja poprawności adresu e-mail nadawcy.

**7. Funkcje modułu Sandbox (Antymalware):**

1) Analiza dynamiczna w maszynach wirtualnych i wykrywanie w załącznikach ataków nie może opierać się na analizie w rozwiązaniach typu chmurowego (poza infrastrukturą Odbiorcy), lecz na urządzeniu zainstalowanym w infrastrukturze Odbiorcy. Analiza ataku musi odbywać się za pomocą dynamicznej analizy zachowania kodu umożliwiającemu równoczesną analizę zagrożenia w różnych wersjach systemu operacyjnego i aplikacjach.
2) Architektura Modułu AntyMalware musi składać się z Centralnego serwera zarządzania modułu AntyMalware, służącego do konfiguracji Modułu, zarządzania politykami bezpieczeństwa dodatkowej ochrony poczty elektronicznej i raportowania oraz Analizatorów dynamicznych służących do wykonywania głębokiej analizy w piaskownicy (sandbox) w środowisku maszyn wirtualnych oraz wykrywania zawansowanych zagrożeń poczty elektronicznej oraz pracujących w trybie MTA (ang. Mail Transfer Agent).
3) Każdy Analizator dynamiczny musi być dostarczony w postaci urządzenia fizycznego Producenta. Urządzenie musi działać w oparciu o dedykowane platformy sprzętowe (appliance) dostarczane przez Producenta rozwiązania z systemem operacyjnym utwardzonym (hardening) przez Producenta.
4) Analizatory dynamiczne modułu AntyMalware muszą działać w postaci klastra.
5) Integracja z posiadanym serwerem centralnego zarządzania musi umożliwiać przynajmniej zarządzanie alertami pochodzącymi z analizatorów dynamicznych, możliwość zwalniania z kwarantanny zatrzymanych wiadomości, zarządzanie politykami bezpieczeństwa na wszystkich klastrach analizatorów jednocześnie i możliwość wykonywania bezpośredniej aktualizacji oprogramowania analizatorów.

6) Moduł Antymalware musi umożliwiać uruchomienie min. 16 instancji wirtualnych systemów MS Windows zawierających Windows 10 i Windows 11 oraz 1 pakiet biurowy MS Office 2019 oraz MS Office 2021 w celu wykonania analizy Sandbox w wymiarze minimum 8 tys. przychodzących wiadomości email na godzinę, w tym minimalnie 400 unikalnych załączników do email na godzinę.
7) Moduł Antymalware musi umożliwiać sprawdzanie procesów i rejestru, połączenia z Botnet C&C oraz złośliwymi URL, dostęp do pakietów przeprocesowanych przez VM, logów działania badanego oprogramowania oraz zrzutów ekranu w badanej VM.
8) Musi umożliwiać Sanboxing dla plików zarchiwizowanych (.tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj), wykonywalnych (.exe, .dll), PDF, Windows Office Document, Javascript, AdobeFlash oraz JavaArchive (JAR), plików multimedialnych: .avi, .mpeg, .mp3, .mp4.
9) Moduł Antymalware musi umożliwiać skanowanie protokołów sieciowych: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM oraz ich wersje zaszyfrowane SSL. Jeżeli do spełnienia tego wymagania konieczne jest dostarczenie dodatkowych urządzeń sieciowych (przekierowujących zawartość pakietów dla wskazanych protokołów sieciowych, rozszywających ruch SSL), urządzenia te wówczas muszą zostać uwzględnione w wysokości oferty. Ich wydajność powinna umożliwiać procesowanie ruchu o przepływności min. 4 Gbps.
10) Moduł AntyMalware musi być zoptymalizowany pod kątem minimalizacji ilości przypadków false-positive (błędne wykrycie zagrożenia w poprawnej wiadomości email).
11) Moduł AntyMalware musi posiadać dodatkowy mechanizm wykrywający obiekty lub zdarzenia, które mogą wskazywać, że są elementem ataku:
    a. skrypty przesyłane w wiadomości email,
    b. pliki wykonywalne przesyłane w załączniku lub URL,
    c. dokumenty MS OFFICE z zaimplementowanym makro lub kodem wykonywalnym,
    d. nietypowych załączników przesyłanych w wiadomości takich jak: BAT, CPL, LNK, COM, CMD, MHT, PIF, PUB, HLP, HTA, ISO,
    e. wiadomości email ze skróconymi linkami (tiny URL),
    f. dokumenty MS OFFICE z flash,
    g. pliki JAR,
    h. hasła z formularzy przesyłanych w formie HTTP request,
    i. zaszyfrowane pliki PDF,
    j. nieznanych plików konfiguracyjnych .SettingContent-ms.
    k. zaszyfrowane dokumenty MS Office
    l. Dokumenty MS Office z obiektami Embedded Object
    m. Dokumenty PDF, HWP lub MS Office z aktywnością sieciową
    n. pliki MS Office z makrem tworzącym plik wykonywalny
    o. uszkodzone pliki wykonywalne PE
    p. obiekty próbujące wykryć rozwiązania AV/Firewall za pomocą WMI
    q. pliki z niezgodnym rozszerzeniem (innym niż w magic byte)
    r. dokumenty Office z zagnieżdżonymi obiektami SWF

12) Moduł AntyMalware musi mieć możliwość przepisania adresów URL w przesyłanej wiadomości tak aby pomimo kliknięcia użytkownik nie był przekierowany do potencjalnie złośliwej treści. W wypadku kiedy adres URL będzie złośliwy, przedstawiony ekran informujący o blokadzie musi umożliwiać dostosowanie prezentowanych użytkownikowi komunikatów do wymagań Odbiorcy (grafika i tekst z informacją o blokadzie w języku Polskim).
13) Moduł AntyMalware musi posiadać mechanizm ekstrakcji (rozpoznawania) adresów URL z załączników przesyłanych w wiadomości email i możliwość detonowania ich w środowisku wirtualnym w przypadku pliku zlokalizowanego w URL.
14) Moduł Antymalware musi umożliwiać skanowanie stron www z linkami URL.
15) Moduł Antymalware musi posiadać czarne i białe listy dla sum kontrolnych plików.
16) Moduł Antymalware musi umożliwiać szczegółowe raportowanie charakterystyki badanego pliku oraz zachowania: modyfikacji plików w systemie, zachowania uruchomionych procesów, zmian w rejestrze, zachowania sieci, snapshotu VM.
17) Moduł Antymalware musi umożliwiać dostęp do analizowanych plików w celu dodatkowego badania: przykładowe pliki, logi z analizy (tracer), zapis pakietów pcap.
18) Moduł Antymalware musi wspierać możliwość ręcznego skanowania plików poprzez ich „wrzucenie" do systemu z innych źródeł niż poczta elektroniczna.
19) Moduł Antymalware musi posiadać możliwość wykorzystania maszyny VM Windows, która jest obrazem maszyny Zamawiającego.
20) Zarządzanie Modułem poprzez lokalny graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS oraz dostęp do CLI przez SSH.
21) Moduł AntyMalware musi dodawać oznaczenia (X header) do nagłówków wiadomości email zależnie od akcji podjętej przez Moduł analizy (m.in. email przeskanowany bez wykrytego zagrożenia, email zawiera kod złośliwy) do wykorzystania przez inne systemy ochrony Odbiorcy i analizy wstecznej.
22) Moduł AntyMalware musi być zoptymalizowany pod kątem minimalizacji ilości przypadków false-positive (błędne wykrycie zagrożenia w poprawnej wiadomości email).

**8. Funkcje logowania i raportowania modułu ochrony poczty (Antyspam):**

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1) Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
2) Logowanie informacji na temat spamu oraz niedozwolonych załączników.
3) Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
4) Możliwość analizy przebiegu sesji SMTP.
5) Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
6) Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
7) Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

**9. Wymagania w zakresie wdrożenia:**

1) Urządzenia muszą być fabrycznie nowe, nieużywane wcześniej, muszą być objęte opieką serwisową producenta oraz posiadać najnowszą dostępną stabilną wersję oprogramowania.
2) Urządzenia muszą być dostarczone ze wszystkimi niezbędnymi do działania i zapewnienia wymaganych funkcjonalności licencjami na używanie tych funkcjonalności.
3) W ramach wdrożenia Systemu Wykonawca dostarczy, zainstaluje i skonfiguruje System, zgodnie z założeniami Zamawiającego.
4) Wdrożenie Środowiska realizowane będzie przez autoryzowanych inżynierów posiadających certyfikat maksymalnie o jeden poziom niższy od najwyższego na ścieżce certyfikacyjnej producenta, uprawniający do realizacji prac. Wykonawca załączy certyfikat poświadczający spełnienie warunku na etapie składania ofert.
5) W celu zapewnienia wymaganego poziomu jakości wdrożenia ora wsparcia systemu Wykonawca musi posiadać status partnera producenta oprogramowania lub sprzętu z zastrzeżeniem, że jeśli producent stosuje kilka poziomów partnerstwa, Zamawiający wymaga, aby Wykonawca posiadał poziom partnerstwa nie niższy niż drugi w kolejności licząc od najwyższego poziomu partnerstwa w hierarchii poziomów partnerstwa stosowanej przez producenta.
6) Zamawiający zastrzega, że wszystkie podawane parametry, o ile nie zostało to wskazane inaczej należy traktować jako parametry minimalne.
7) Potwierdzeniem prawidłowej realizacji przedmiotu umowy w zakresie uruchomienia i skonfigurowania Systemu będzie podpisany bez zastrzeżeń Protokół Odbioru Wdrożenia Systemu (zgodnie z postanowieniami Projektowanych postanowień umowy) zawierający w szczególności odbiór Systemu ochrony poczty elektronicznej wraz z wchodzącymi w skład Systemu Modułami ochrony, na podstawie przeprowadzonych Testów Akceptacyjnych oraz potwierdzajcy przeprowadzenie szkoleń.

**10. Wsparcie producenta musi zapewniać:**

1) Dostęp do poprawek i nowych wersji dla oprogramowania i funkcji zaimplementowanych w ramach wdrożenia;
2) Dostęp do bazy wiedzy, szkoleń oraz innych materiałów producenta dotyczących eksploatacji systemu,
3) Zgłaszanie awarii do serwisu producenta oraz rozwiązywanie problemów.

**11. Wymagania w zakresie szkolenia:**

1) Zamawiający wymaga przeprowadzenia **szkolenia minimum dla 4** administratorów Zamawiającego przez **minimum 8 godzin rozłożonych na co najmniej 2 dni.** Szkolenie zostanie przeprowadzone przez Wykonawcę w terminie do 10 dni roboczych od daty podpisania umowy w terminie uzgodnionym z Zamawiającym.
2) Szkolenie przeprowadzone przez Wykonawcę ma na celu naukę administratorów w zakresie:
   a) prawidłowego i bezpiecznego korzystania z Systemu,
   b) tworzeniu ról i reguł w Systemie,
   c) zarządzania uprawnieniami, definicjami oraz użytkownikami,
   d) automatycznych instalatorów aplikacji,
   e) administrowanie systemu,

3) Szkolenie administratorów Zamawiającego musi być świadczone w języku polskim.

**12. Wymagania w zakresie wsparcia technicznego:**

1) Wykonawca zobowiązuje się zapewnić wsparcie techniczne Systemu świadczone w języku polskim przez minimum 36 miesięcy od dnia wdrożenia Systemu (potwierdzonego protokołem odbioru), w dni robocze w godzinach pracy UOKiK: 08:00 - 17:00 zgodnie z wymaganiami szczegółowo określonymi w umowie.