Opis Przedmiotu Zamówienia

Zakup oprogramowania dla podniesienia bezpieczeństwa systemu pocztowego statystyki publicznej.

Przedmiotem zamówienia jest dostawa oprogramowania, w tym maszyn wirtualnych typu VA (*virtual applian*ce) wraz z licencjami i trzyletnim wsparciem producenta oraz wykonanie wdrożenia dostarczonych komponentów w infrastrukturze Zamawiającego w Podstawowym Centrum Przetwarzania Danych.

W szczególności przedmiot zamówienia obejmuje następujące zadania do realizacji przez Wykonawcę:

1. Dostawa oraz wdrożenie oprogramowania, w tym urządzeń wirtualnych do zabezpieczenia transmisji wejściowych i wyjściowych danych pocztowych oraz zewnętrznych serwerów systemu pocztowego statystyki publicznej wraz z licencjami oraz trzyletnim wsparciem producenta na cały system zwany dalej SOSZ (Systemem ochrony serwerów zewnętrznych) dla 6500 użytkowników lub 7500 skrzynek pocztowych w zależności od sposobu licencjonowania dostarczonego oprogramowania.
2. Dostawa oraz wdrożenie oprogramowania do zabezpieczenia wewnętrznych serwerów pocztowych wraz z licencjami oraz trzyletnim wsparciem producenta na cały system zwany dalej SOSW (Systemem ochrony serwerów wewnętrznych) dla 6500 użytkowników lub 7500 skrzynek pocztowych w zależności od sposobu licencjonowania dostarczonego oprogramowania.
3. Przeprowadzenie szkoleń.

I. Wspólne uwarunkowania dla zadań oraz opis środowiska Zamawiającego

Prace wdrożeniowe i konfiguracyjne będą realizowane w Podstawowym Centrum Przetwarzania Danych mieszczącym się w siedzibie Zamawiającego w Warszawie.

Z uwagi na fakt, iż prace wdrożeniowe i rekonfiguracyjne będą prowadzone na działającym środowisku sprzętowo–systemowo–aplikacyjnym, wymagane jest zachowanie ciągłości działania tego środowiska, minimalizacja przestojów, szczegółowe zaplanowanie wszelkich prac oraz przygotowanie scenariuszy awaryjnych.

1. Zamawiający posiada domenę produkcyjną AD DS. (MS Active Directory) Windows Serwer 2012R2 o funkcjonalności lasu i domeny na poziomie Windows Server 2008R2.
2. Poczta korporacyjna statystyki publicznej działa w oparciu o MS Exchange Server 2010 SP3 RU 8v2. System pocztowy jest scentralizowany – wszystkie serwery pocztowe znajdują się w Podstawowym Centrum Przetwarzania Danych.
3. System poczty elektronicznej składa się z 7 serwerów:
    a. 3 serwerów MS Exchange Mailbox Server Role, spiętych w klaster wysokiej dostępności DAG (*Database Availability Group*).
    b. 2 serwerów MS Exchange Hub Transport Server Role wraz z Client Access Server Role, działających w klastrze NLB.
    c. 2 serwerów MS Exchange Edge Transport Server Role.
4. Na serwerach pocztowych zainstalowany jest system operacyjny MS Windows Server 2008 R2.
5. Zamawiający dysponuje środowiskiem do wirtualizacji serwerów zbudowanym w oparciu o oprogramowanie VMware vCenter 5.1.
6. Do obsługi baz technicznych Zamawiający wykorzystuje oprogramowanie MS SQL Server 2008 oraz 2012 Standard Edition.
7. Do ochrony zewnętrznego ruchu pocztowego Zamawiający wykorzystuje oprogramowanie McAfee Email Gateway 7.6.

8. Do ochrony wewnętrznych serwerów pocztowych Zamawiający wykorzystuje oprogramowanie ESET Mail Security for Microsoft Exchange 6.4.

II. Opis infrastruktury sprzętowo-systemowej posiadanej przez Zamawiającego i dedykowanej dla wdrożenia

1. Zamawiający udostępni do dyspozycji Wykonawcy możliwość tworzenia niezbędnej liczby maszyn wirtualnych w środowisku VMware vCenter 5.1 wraz z licencjami serwerowymi MS Windows 2008 R2 lub 2012 R2, będącymi w posiadaniu Zamawiającego.
2. Do utworzenia niezbędnych baz technicznych Zamawiający udostępni klaster MS SQL Server 2008 lub 2012 Standard Edition posiadany przez Zamawiającego.

W przypadku zaoferowania systemu, który nie będzie wykorzystywał udostępnionych przez Zamawiającego zasobów i posiadanych licencji, Wykonawca dostarczy wszystkie niezbędne elementy sprzętowe, systemowe i aplikacyjne.

III. Wymagania dotyczące bezpieczeństwa dostarczonego oprogramowania

Dostarczone oprogramowanie nie może być zabronione do stosowania przez administrację którekolwiek z Państw członkowskich NATO (North Atlantic Treaty Organization).

IV. Szczegółowa specyfikacja i opisy zadań do realizacji przez Wykonawcę

Wykonawca przeprowadzi szczegółową analizę obecnie funkcjonującej infrastruktury systemu pocztowego Zamawiającego przeznaczonej do zabezpieczenia oraz opracuje i uzgodni z Zamawiającym koncepcję i harmonogram realizacji poszczególnych zadań.

Zadanie 1. Dostawa oraz wdrożenie oprogramowania, w tym urządzeń wirtualnych do zabezpieczenia transmisji wejściowych i wyjściowych danych pocztowych oraz zewnętrznych serwerów systemu pocztowego statystyki publicznej wraz z licencjami oraz trzyletnim wsparciem producenta na cały system zwany dalej SOSZ (Systemem ochrony serwerów zewnętrznych) dla 6500 użytkowników lub 7500 skrzynek pocztowych w zależności od sposobu licencjonowania dostarczonego oprogramowania.

Przedmiotem zadania jest dostawa oraz wdrożenie oprogramowania oraz urządzeń wirtualnych wraz z licencjami oraz trzyletnim wsparciem producenta pozwalającym na pobieranie aktualnych plików sygnatur, baz danych opisujących ataki, baz kategorii URL, instalację nowych wersji oprogramowania i korzystanie z pomocy technicznej.

1. Wymagania ogólne w zakresie licencji SOSZ

Licencje mogą być dostarczone w pakiecie zawierającym wymagane funkcjonalności lub jako samodzielne produkty, ale muszą pochodzić od tego samego producenta. Zamawiający wymaga trzyletniego wsparcia producenta na dostarczone oprogramowanie. Licencje muszą pozwalać na swobodne przenoszenie pomiędzy maszynami wirtualnymi. **Dostarczone licencje muszą umożliwiać wdrożenie co najmniej dwóch VA (*virtual applian*ce) lub większej liczby maszyn VA, jeśli dostarczone rozwiązanie tego wymaga, w celu zapewnienia obsługi poczty nawet w przypadku awarii jednego z elementów.**

2. Podstawowe wymagania funkcjonalne SOSZ

a. Wdrożone rozwiązanie ma obsługiwać 6500 użytkowników lub 7500 skrzynek pocztowych Zamawiającego w zależności od sposobu licencjonowania dostarczonego oprogramowania.
b. System musi umożliwić ochronę ruchu pocztowego na poziomie co najmniej 8000 e-maili przychodzących i 8000 e-maili wychodzących dziennie *per* serwer brzegowy.

c. System musi pracować w trybie bramki pocztowej SMTP.
d. Rozwiązanie ma działać w warstwie sieciowej i musi obsługiwać co najmniej protokół SMTP, przy czym musi być możliwe określenie portów na jakich działa protokół.
e. System musi zapewnić zintegrowaną ochronę antyspamową, antywirusową oraz filtrowanie treści.
f. System musi posiadać wbudowane wydajne mechanizmy ograniczania skutków ataków typu DoS (*Denial of Service*) z wykorzystaniem poczty elektronicznej.
g. System ma zapewniać ochronę *anti-relay*.
h. System ma być zbudowany w oparciu o maszyny wirtualne typu VA kompatybilne z VMware vCenter w wersji 5.1 i nowszej.
i. Rozwiązanie powinno umożliwiać wdrożenie maszyn wirtualnych typu VA w konfiguracji *proxy* aplikacyjnego (*mail relay*).
j. System musi być zbudowany w oparciu o elementy zapewniające wysoką dostępność, umożliwiające obsługę poczty nawet w wypadku awarii jednego z elementów systemu oraz mechanizmy pozwalające na rozłożenie obciążenia pomiędzy urządzeniami wirtualnymi VA.
k. System musi umożliwiać centralne zarządzanie wieloma maszynami wirtualnymi typu VA bez konieczności zakupu dodatkowych licencji lub oprogramowania.
l. Zarządzanie powinno odbywać się poprzez standardową przeglądarkę WWW i połączenie https.
m. Interfejs zarządzający musi umożliwiać wizualizację przebiegu sesji protokołu SMTP i przejścia wiadomości przez poszczególne filtry ochronne.
n. System musi posiadać wbudowane raportowanie, bez konieczności stosowania dodatkowego oprogramowania i zewnętrznych serwerów.
o. System musi umożliwiać importowanie bazy kont z serwerów LDAP w tym AD DS.
p. System musi pozwalać na autentykację odbiorcy poczty i stworzenie polityki skanowania poczty uzależnionej od grup użytkowników lub poszczególnych użytkowników pochodzących z systemu poczty korporacyjnej statystyki publicznej.
q. Oprogramowanie musi pozwalać na stworzenie polityki skanowania zależnie od nazwy lub adresu IP domeny pocztowej, adresu źródłowego/docelowego użytkownika lub grupy użytkowników.
r. Musi być możliwe tworzenie osobnych polityk dla wiadomości wychodzących i dla przychodzących.
s. Musi być możliwe definiowanie równocześnie wielu polityk, których zastosowanie zależy od kolejności na liście polityk i w/w kryteriów.
t. Konfigurowanie polityk musi umożliwiać definiowanie kilku jednoczesnych reakcji na wykryte zdarzenie w tym na:
    i. Zablokowanie wiadomości i wysłanie powiadomienia o tym zdarzeniu pod wskazany adres email.
    ii. Zablokowanie wiadomości i skierowanie jej do kwarantanny.
    iii. Przesłanie poczty do odbiorcy wraz z modyfikacją nagłówka wiadomości.
u. System musi usuwać z nagłówków wiadomości pocztowych informacje dotyczące wewnętrznej infrastruktury Zamawiającego.
v. Rozwiązanie, w ramach zdefiniowanych polityk, musi umożliwiać ograniczanie:
    i. Maksymalnej wielkości przesyłki pocztowej.
    ii. Maksymalnej wielkości załącznika.
    iii. Maksymalnej liczby załączników.
w. System musi umożliwiać konfigurowanie polityk w zależności od rozmiaru, nazwy, typu oraz rozszerzenia załącznika.

x. System musi umożliwiać filtrowanie poczty na podstawie zawartości przesyłek (treści, załączników, atrybutów) w oparciu o słowa kluczowe, reguły, szablony, wbudowane i tworzone przez administratora słowniki.
y. System musi umożliwiać szyfrowanie poczty elektronicznej korzystając z technologii TLS, S/MIME.
z. W ramach oferowanego systemu należy zapewnić rozwiązanie do centralnej, wspólnej obsługi kwarantanny ze wszystkich działających w sieci urządzeń wirtualnych VA.
aa. Interfejs zarządzający musi umożliwiać administratorowi zarządzanie wiadomościami przechowywanymi w centralnej kwarantannie.
bb. Decyzja o przesłaniu wiadomości do kwarantanny musi wynikać z definicji działania poszczególnych filtrów: antywirusowego, antyspamowego lub weryfikacji treści.
cc. System musi umożliwiać tworzenie wielu kont administracyjnych z różnymi poziomem uprawnień.
dd. Rozwiązanie musi pozwalać na logowanie aktywności użytkowników systemu.
ee. Rozwiązanie musi posiadać wbudowane mechanizmy pozwalające na wysyłanie powiadomień o stanie pracy poszczególnych komponentów systemu.
ff. System musi pozwalać na integrację z systemem analizy zagrożeń typu *on-premise Sandbox*. Integracja powinna polegać co najmniej na możliwości wysyłania do analizy podejrzanych wiadomości, w tym załączników.

3. Wymagania funkcjonalne SOSZ w zakresie ochrony antywirusowej

a. System musi być wyposażony w skaner AV (antywirusowy) pochodzący od tego samego producenta, co całe oferowane rozwiązanie.
b. Skaner AV musi wykorzystywać dzienne, automatyczne aktualizacje baz sygnatur antywirusowych. Musi istnieć możliwość określenia częstotliwości i harmonogramu aktualizacji silnika AV i baz sygnatur.
c. Skaner AV musi posiadać mechanizm wykrywający nowe zagrożenia za pomocą internetowych serwisów reputacyjnych zarządzanych przez producenta rozwiązania. W razie wykrycia podejrzanego kodu/pliku i braku definicji w lokalnym pliku sygnatur antywirusowych, skaner AV musi mieć możliwość wysłania zapytania do centralnej bazy prowadzonej przez producenta.
d. Skaner AV musi wykrywać i blokować oprogramowanie szpiegujące oraz wykrywać próby ataków typu *phishing*.
e. Skaner AV musi wykrywać wykorzystanie mechanizmów kompresji używanych przez szkodliwe oprogramowanie i musi umożliwiać automatyczne skasowanie plików przygotowanych z ich użyciem.
f. Skaner AV musi umożliwiać blokowanie skryptów, apletów Java oraz ActiveX.

4. Wymagania funkcjonalne SOSZ w zakresie ochrony antyspamowej

a. System musi zapewniać ochronę przed spamem – powinien być wyposażony w moduł antyspamowy (AS) pochodzący od tego samego producenta, co całe oferowane rozwiązanie.
b. Skaner AS musi działać w oparciu o system oceny prawdopodobieństwa wystąpienia spamu bazujący na regułach aktualizowanych przez producenta.
c. Aktualizacja reguł musi odbywać się na bieżąco kilka razy na godzinę, a co najmniej raz dziennie.

d. System AS musi mieć możliwość wysyłania wiadomości do internetowego serwisu reputacyjnego producenta w celu dalszej weryfikacji dodatkowymi mechanizmami antyspamowymi.
e. Skaner AS musi współpracować z serwerami AD DS i LDAP, posiadanymi przez Zamawiającego, pozwalając na stworzenie polityki skanowania zależnie od adresu pocztowego, grupy użytkowników w AD DS/LDAP, domeny pocztowej lub zakresu IP.
f. System AS musi obsługiwać białe i czarne listy (*blacklist* i *whitelist*) definiowane przez administratora.
g. System AS musi obsługiwać serwery RBL zarządzane przez producenta rozwiązania. Musi być także możliwe definiowanie dodatkowych źródeł RBL przez administratora systemu.
h. System AS musi wykrywać i blokować ataki typu *directory harvest.*
i. System AS musi obsługiwać technologie *graylisting*, SPF oraz *Sender ID.*
j. System AS musi chronić przed spamem generowanym za pomocą mechanizmu potwierdzania problemów z doręczeniem przesyłki (NDR).
k. System powinien wykorzystywać funkcję FCrDNS realizującą sprawdzenie poprawności konfiguracji rozwiązywania nazw DNS systemu nadającego wiadomość.
l. System AS musi posiadać filtr reputacyjny badający domenę i adres IP, z których nadana została wiadomość oraz zawartość przesyłaną w email.
m. Musi być możliwe takie skonfigurowanie polityki ochrony antyspamowej, aby już sam wynik z serwisu reputacyjnego (niska reputacja nadawcy) powodował odrzucenie email lub skierowanie go do kwarantanny.
n. Musi być także możliwe uwzględnienie wyników z serwisu reputacyjnego w całościowej ocenie prawdopodobieństwa wykrycia spamu i podejmowanie decyzji o losie przesyłki na podstawie końcowego wyniku analizy, po przejściu email przez inne filtry analizujące wiadomość.
o. System powinien umożliwiać badanie reputacji URL w treści wiadomości i filtrować wiadomość z URL o złej reputacji.
p. Musi być możliwe zdefiniowanie różnych akcji podejmowanych po wykryciu spamu zależnie od określonego przez system prawdopodobieństwa wykrycia spamu (*spam score*):
    i. Zablokowanie i skasowanie wiadomości z powiadomieniem końcowego użytkownika, a także bez takiego powiadomienia (zależnie od przyjętej polityki).
    ii. Przekazanie wiadomości do kwarantanny.
    iii. Przesłanie wiadomości do odbiorcy z oznakowaniem jej jako spam w tytule wiadomości.
    iv. Dodanie do nagłówka wiadomości informacji o prawdopodobieństwie wystąpienia spamu.
    v. Dodanie do nagłówka wiadomości informacji, które reguły antyspamowe spowodowały wykrycie spamu.

5. Wymagania projektowe i szczegółowa specyfikacja prac

W ramach przedmiotu umowy Wykonawca wykona następujące prace:

a. Przygotuje **Projekt techniczny** realizacji uzgodnionej koncepcji uwzględniający dobre praktyki i rekomendacje eksploatacyjne publikowane przez producenta oprogramowania.
b. Przygotuje koncepcję realizacji zadania.
c. Opracuje i uzgodni szczegółowy harmonogram realizacji prac uwzględniający specyfikę organizacji Zamawiającego.
d. Wdroży i skonfiguruje według zaakceptowanego Projektu technicznego dostarczone

oprogramowanie oraz maszyny wirtualne typu VA do ochrony zewnętrznych serwerów pocztowych.

e. Wykona niezbędną konfigurację sieciową i integrację z systemem pocztowym Zamawiającego.
f. Dokona migracji lub wymiany komponentów obecnego używanego systemu ochrony poczty korporacyjnej Zamawiającego.
g. Skonfiguruje polityki konfiguracyjne z wykorzystaniem najlepszych praktyk producenta oprogramowania dla wdrożonych produktów.
h. Opracuje scenariusze testowe i przeprowadzi testy akceptacyjne wdrożonego rozwiązania.
i. Opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy.
j. Wykonawca opracuje **Dokumentację powykonawczą**, która będzie zawierać:
    i. Opis architektury zaimplementowanego rozwiązania.
    ii. Szczegółowy opis instalacji i konfiguracji wykorzystywanego oprogramowania, ze wskazaniem wybranych opcji i ustawionych wartości.
    iii. Konfigurację poszczególnych modułów, komponentów i usług.
    iv. Zbiór zaimplementowanych polityk konfiguracyjnych dla poszczególnych modułów.
    v. Politykę i procedury wykonywania kopii zapasowych.
    vi. Szczegółowe procedury eksploatacyjne oraz awaryjnego odtwarzania funkcjonalności systemu, opisujące krok po kroku niezbędne czynności umożliwiające Zamawiającemu samodzielne przywrócenie funkcjonalności systemu.
    vii. Procedury i instrukcje bieżącego monitoringu oraz utrzymania i aktualizacji systemu.

Zamawiający wymaga, aby Dokumentacja powykonawcza napisana była w języku polskim. Wykonawca przekaże Zamawiającemu Dokumentację powykonawczą w trzech egzemplarzach w formie papierowej oraz w formie elektronicznej na nośniku CD. Dokumentacja na nośniku CD musi posiadać format pliku do edycji.

Zadanie 2. Dostawa oraz wdrożenie oprogramowania do zabezpieczenia wewnętrznych serwerów pocztowych wraz z licencjami oraz trzyletnim wsparciem producenta na cały system zwany dalej SOSW (Systemem ochrony serwerów wewnętrznych) dla 6500 użytkowników lub 7500 skrzynek pocztowych w zależności od sposobu licencjonowania dostarczonego oprogramowania.

Przedmiotem zadania jest dostawa oraz wdrożenie oprogramowania wraz z licencjami oraz trzyletnim wsparciem producenta pozwalającym na pobieranie aktualnych baz sygnatur wirusów, instalację nowych wersji oprogramowania i korzystanie z pomocy technicznej.

1. Wymagania ogólne w zakresie licencji SOSW

Licencje mogą być dostarczone w pakiecie zawierającym wymagane funkcjonalności lub jako samodzielne produkty, muszą pochodzić od tego samego producenta**.** Zamawiający wymaga trzyletniego wsparcia producenta na dostarczone oprogramowanie. Licencje muszą pozwalać na swobodne przenoszenie pomiędzy serwerami pocztowymi.

2. Wymagania funkcjonalne SOSW

a. Wdrożone rozwiązanie ma obsługiwać 6500 użytkowników lub 7500 skrzynek pocztowych skrzynek pocztowych Zamawiającego w zależności od sposobu licencjonowania dostarczonego oprogramowania.
b. Ochrona ma być realizowana przez dedykowane oprogramowanie antywirusowe instalowane na platformie serwerów MS Exchange analizujące wiadomości pocztowe przyjmowane przez te serwery.
c. System musi być zgodny z MS Exchange 2010 posiadanym przez Zamawiającego (zgodnie z opisem środowiska Zamawiającego).
d. System musi się integrować z systemem poczty elektronicznej MS Exchange 2010 z

wykorzystaniem przewidzianych przez twórców oprogramowania Exchange do tego celu mechanizmów (interfejsów programowych): VSAPI i Transport Agent.

e. Ochroną antywirusową objęta musi być poczta elektroniczna Zamawiającego na wszystkich etapach transmisji przesyłki pocztowej:
    i. Na etapie przyjmowania/wysyłania przesyłki pocztowej z/do Internetu – na serwerach MS Exchange Edge Server Role.
    ii. Na etapie transportu przesyłki pocztowej - na serwerach MS Exchange Hub Transport Server Role.
    iii. Na etapie składowania przesyłki pocztowej - na serwerach MS Exchange Mailbox Server Role.
f. Sprawdzane antywirusowo muszą być przesyłki zarówno przychodzące jak i wychodzące do/z skrzynki pocztowej użytkownika.
g. Sprawdzanie antywirusowe przesyłek na serwerach transportowych poczty elektronicznej (MS Exchange Hub Transport Server Role, MS Exchange Edge Server Role) musi odbywać się w czasie rzeczywistym nie zakłócając prawidłowego przebiegu przesyłki pocztowej, wykorzystując funkcjonalność *Transport Agent*.
h. Sprawdzanie antywirusowe przesyłek na serwerach skrzynkowych (MS Exchange Mailbox Server Role) musi się odbywać bezpośrednio w storach Exchange:
    i. W momencie dotarcia przesyłki pocztowej na serwer skrzynkowy.
    ii. W momencie pojawienia się nowoutworzonej, przez użytkownika, przesyłki pocztowej.
    iii. Zgodnie z harmonogramem sprawdzania skrzynek pocztowych użytkowników.
    iv. Na żądanie administratora systemu antywirusowego poczty elektronicznej.
i. W przypadku wykrycia szkodliwego pliku/kodu musi istnieć możliwość usunięcia wiadomości/załącznika, wyleczenia, podmiany załącznika na czysty plik zawierający jedynie informację o infekcji.
j. W przypadku wykrycia szkodliwego pliku/kodu wiadomości system musi generować powiadomienia dla administratora systemu.
k. Przesyłki, w których wystąpiło podejrzenie występowania szkodliwej zawartości muszą być składowane w miejscu niedostępnym dla użytkowników poczty (w kwarantannie).
l. Administrator systemu antywirusowego poczty elektronicznej musi mieć możliwość zarzadzania kwarantanną poprzez:
    i. Wgląd do zawartości kwarantanny.
    ii. Usuwanie przesyłek z kwarantanny.
    iii. Zwalnianie przesyłek z kwarantanny – skierowanie przesyłki wcześniej poddanej kwarantannie do adresata.
    iv. Mechanizm kwarantanny musi mieć zabezpieczenie przed przepełnieniem.
m. System musi być zarządzany z jednego miejsca – za pomocą centralnej konsoli administracyjnej.
n. System musi wspierać rozwiązania klastrowe DAG.
o. Oprogramowanie musi korzystać z dziennych uaktualnień sygnatur.
p. System antywirusowy poczty elektronicznej może zawierać dodatkowe funkcjonalności (np. ochronę antyspamową, *anti-phishing*), jeżeli wchodzą w skład zaproponowanego pakietu oprogramowania. Obecność tych funkcjonalności nie jest wymagana.

3. Wymagania projektowe i szczegółowa specyfikacja prac

W ramach przedmiotu umowy Wykonawca wykona następujące prace:

a. Przygotuje koncepcję realizacji zadania.
b. Opracuje i uzgodni szczegółowy harmonogram realizacji prac uwzględniający specyfikę organizacji Zamawiającego.
c. Wdroży i skonfiguruje dostarczone oprogramowanie do ochrony wewnętrznych serwerów pocztowych.

d. Dokona migracji lub wymiany komponentów obecnego używanego systemu ochrony poczty korporacyjnej Zamawiającego.
e. Skonfiguruje polityki konfiguracyjne z wykorzystaniem najlepszych praktyk producenta oprogramowania dla wdrożonych produktów.
f. Opracuje scenariusze testowe i przeprowadzi testy akceptacyjne wdrożonego rozwiązania.
g. Opracuje i przedstawi raport z testów. W przypadku zrealizowania scenariusza testowego z wynikiem negatywnym, Wykonawca przedstawi nowe rozwiązanie wadliwego elementu systemu i przeprowadzi ponowny test wg scenariusza w terminie wyznaczonym przez Zamawiającego, dochowując terminu wykonania Umowy.
h. Wykonawca opracuje **Dokumentację powykonawczą**, która będzie zawierać:
    i. Opis architektury zaimplementowanego rozwiązania.
    ii. Szczegółowy opis instalacji i konfiguracji wykorzystywanego oprogramowania, ze wskazaniem wybranych opcji i ustawionych wartości.
    iii. Konfigurację poszczególnych modułów, komponentów i usług.
    iv. Zbiór zaimplementowanych polityk konfiguracyjnych dla poszczególnych modułów.
    v. Szczegółowe procedury eksploatacyjne oraz awaryjnego odtwarzania funkcjonalności systemu, opisujące krok po kroku niezbędne czynności umożliwiające Zamawiającemu samodzielne przywrócenie funkcjonalności systemu.
    vi. Procedury i instrukcje bieżącego monitoringu oraz utrzymania i aktualizacji systemu.

Zamawiający wymaga, aby Dokumentacja powykonawcza napisana była w języku polskim. Wykonawca przekaże Zamawiającemu Dokumentację powykonawczą w trzech egzemplarzach w formie papierowej oraz w formie elektronicznej na nośniku CD. Dokumentacja na nośniku CD musi posiadać format pliku do edycji.

Zadanie 3. Przeprowadzenie szkoleń

1. Wykonawca przeprowadzi szkolenia zgodnie z następującymi wymaganiami:
    a. **Szkolenie dla administratorów SOSZ**
        i. 4 osoby,
        ii. czas trwania szkolenia: 3 dni robocze (24 godziny zegarowe),
    b. **Szkolenie dla administratorów SOSW**
        i. 4 osoby,
        ii. czas trwania szkolenia: 2 dni robocze (16 godzin zegarowych),
    c. Program szkolenia – instalacja i konfiguracja komponentów wdrożonego rozwiązania ze szczególnym uwzględnieniem konfiguracji polityk poszczególnych modułów.
    d. Szkolenie musi mieć formę wykładów i warsztatów.
    e. Wszyscy uczestnicy szkolenia muszą otrzymać materiały szkoleniowe w języku polskim lub angielskim, w formie papierowej lub elektronicznej w formacie PDF.
    f. Wszyscy uczestnicy szkolenia otrzymają zaświadczenia potwierdzające ukończenie szkolenia i posiadania odpowiednich kompetencji administratora.
    g. Wykonawca pokryje wszelkie koszty związane z dojazdem, wyżywieniem, pobytem oraz zakwaterowaniem uczestników kursu jeśli szkolenie będzie odbywać się poza Warszawą.
    h. Wykonawca każdego dnia trwania szkolenia zapewni dla wszystkich uczestników: dwie przerwy kawowe, każda trwająca ok. 10 minut oraz jedną przerwę obiadową trwającą ok. 40 minut.

i. W przypadku szkoleń poza Warszawą Wykonawca zapewni uczestnikom szkolenia - 3 posiłki dziennie, w tym obiad oraz napoje i drobne przekąski w czasie przerw (kawa, herbata, woda mineralna), w przypadku szkoleń w Warszawie – 1 ciepły posiłek (obiad) oraz napoje i przekąski w czasie przerw.

j. Wykonawca pokryje wszelkie koszty związane z dojazdem, pobytem oraz wyżywieniem i zakwaterowaniem wykładowców, którzy będą prowadzili szkolenie.

2. 14 dni od daty podpisania Umowy Wykonawca przedstawi Zamawiającemu do akceptacji – harmonogram szkoleń przygotowany w porozumieniu z Zamawiającym obejmujący:
   a. program szkoleń zawierający szczegółowe informacje o zakresie tematycznym i rozkładzie zajęć,
   b. metodę prowadzenia szkoleń,
   c. listę i informacje o wykładowcach, którzy przeprowadzą poszczególne szkolenia.
3. Wykonawca zobowiązany będzie do przeprowadzenia szkoleń zgodnie z zatwierdzonym przez Zamawiającego szczegółowym zakresem tematycznym i harmonogramem szkoleń.
4. Wykonawca w ramach prowadzonych szkoleń zobowiązany jest przekazać Zamawiającemu:
   a. materiały szkoleniowe,
   b. listy obecności,
   c. listę wydanych zaświadczeń i komplet imiennych zaświadczeń dla wszystkich uczestników, którzy ukończą szkolenia, pod warunkiem uczestnictwa w pełnym wymiarze zajęć.