SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA
zwany dalej „SOPZ”
(SPECYFIKACJA TECHNICZNA)
CZĘŚĆ I

Przedmiotem zamówienia jest rozbudowa aktualnie użytkowanego u Zamawiającego systemu poczty elektronicznej opartego o rozwiązanie firmy Fortinet (w skład którego wchodzi klaster urządzeń FortiMail 200D pracujących w trybie Gateway oraz maszyna wirtualna FortiMail VM02 pracująca w trybie serwer) o kolejny serwer systemu poczty elektronicznej w postaci maszyny wirtualnej wraz z wdrożeniem oraz szkoleniem dla regionalnych dyrekcji ochrony środowiska.

1. Oferowany produkt musi spełniać wszystkie parametry określone w niniejszym załączniku oraz być fabrycznie nowy, oznakowany symbolem CE tam gdzie jest to wymagane, pochodzić z legalnego źródła, musi być dostarczony przez autoryzowany kanał sprzedaży producenta na terenie kraju i objęty standardowym pakietem usług gwarancyjnych, zawartych w cenie oprogramowania, świadczonych przez sieć serwisową producenta na terenie Polski. Zamawiający zastrzega sobie prawo do żądania potwierdzenia źródła pochodzenia produktu w postaci oświadczenia producenta.
2. Wykonawca musi przedstawić nazwę producenta i nazwę oprogramowania oferowanego systemu.
3. Wszystkie opisane funkcjonalności są wymaganiami minimalnymi.

Dostarczony system musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza. Wymagane jest aby elementy wchodzące w skład systemu ochrony poczty elektronicznej były zrealizowane w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia.

Zamawiający wymaga aby dostarczony system poczty elektronicznej umożliwiał stworzenie klastra wysokiej dostępności (klaster HA) z aktualnie użytkowaną maszyną wirtualną FortiMail VM02.

Dla systemu ochrony poczty elektronicznej obsługującego regionalne dyrekcje ochrony środowiska, Wykonawca zapewni wszystkie poniższe funkcjonalności:

1. **Architektura systemu ochrony** - system ochrony musi zapewniać kompleksową ochronę antyspamową, antywirusową i antyspyware’ową. Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony Wykonawcy wymaga się, aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny pochodziły od jednego producenta, który udzieli Zamawiającemu licencji bez limitu chronionych użytkowników (licencja na urządzenie). System musi być dostarczony w postaci komercyjnej platformy działającej w środowisku wirtualnym aktualnie użytkowanym u Zamawiającego z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESXi/ESX 4.0/4.1/5.0/5.1/5.5/6.0.
2. **System operacyjny** - dla zapewnienia wysokiej sprawności i skuteczności działania systemu ochrony poczty elektronicznej musi on pracować w oparciu o dedykowany

system operacyjny. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia.

3. **Parametry systemu** – system, w ramach dostarczonej licencji, musi zapewnić obsługę co najmniej 4 interfejsów Ethernet 10/100/1000 Base-TX, obsługę powierzchni dyskowej co najmniej 5 TB z możliwością rozszerzenia do 8 TB oraz obsługę pamięci operacyjnej co najmniej 8 GB z możliwością rozszerzenia do 16 GB.
4. **Sposoby implementacji** – system musi umożliwiać pracę w następujących trybach: tryb Gateway, tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej) oraz tryb serwera pocztowego (minimum 1700 skrzynek pocztowych z możliwością rozszerzenia do 3000 skrzynek pocztowych w trybie serwera).
5. **Funkcjonalności** - system musi realizować poniższe funkcjonalności w każdym z trzech trybów pracy:
   a. wsparcie dla wielu domen pocztowych,
   b. politykę filtrowania tworzoną w oparciu o adresy mailowe, nazwy domenowe, adresy IP (w szczególności reguła all-all),
   c. email routing oraz zarządzanie kolejkami bazujące na politykach,
   d. ochrona poczty przychodzącej oraz wychodzącej,
   e. granularne, wielowarstwowe polityki wykrywania spamu oraz wirusów,
   f. skanowanie antywirusowe oraz antyspamowe definiowane na użytkownika w oparciu o atrybuty LDAP,
   g. routing poczty (email routing) w oparciu o LDAP,
   h. kwarantanna poczty z dziennym podsumowaniem (możliwość samodzielnego zwalniania plików z kwarantanny przez użytkownika),
   i. dostęp do kwarantanny poprzez WebMail lub POP3,
   j. archiwizacja poczty przychodzącej i wychodzącej, backup poczty do różnych miejsc przeznaczenia,
   k. uwierzytelnianie SMTP w oparciu o protokoły: LDAP, RADIUS, POP3, IMAP,
   l. mechanizmy reputacji nadawcy wiadomości,
   m. whitelist'y definiowane dla użytkownika.
6. **Funkcjonalności w trybie serwera pocztowego** – system musi zapewniać następujące funkcjonalności:
   a. obsługę serwisów pocztowych: SMTP, POP3, IMAP,
   b. wsparcie SMTP over SSL,
   c. definiowanie powierzchni dyskowej dla użytkowników,
   d. szyfrowany dostęp do poczty poprzez WebMail,
   e. polski interfejs użytkownika przy dostępie przez WebMail,
   f. kalendarz na WebMail'u,
   g. lokalne konta użytkowników oraz uwierzytelnianie w oparciu o LDAP,
   h. synchronizacja książki adresowej z LDAP.

7. **Ochrona antywirusowa, antyspyware'owa** – system musi realizować następujące funkcjonalności:
   a. skanowanie antywirusowe wiadomości SMTP,
   b. kwarantannę dla zainfekowanych plików,
   c. skanowanie załączników skompresowanych,
   d. definiowanie komunikatów powiadomień w języku polskim. Blokowanie załączników ze względu na typ pliku.
8. **Ochrona antyspamowa** – system musi zapewniać poniższe metody filtrowania spamu:
   a. heurystyczna analiza poczty z dynamiczną aktualizacją reguł,
   b. filtrowanie treści załączników, filtrowanie wiadomości po słowach kluczowych,
   c. szczegółowa kontrola nagłówka wiadomości,
   d. filtrowanie w oparciu o filtry Bayes'a, z możliwością dostrajania dla poszczególnych użytkowników,
   e. filtrowanie poczty w oparciu o sumy kontrolne spamu,
   f. wykrywanie spamu w oparciu a analizę plików graficznych oraz plików PDF,
   g. analiza poczty w oparciu o dynamiczną bazę spamu dostarczaną przez tego samego producenta,
   h. współpraca z zewnętrznymi serwerami RBL,
   i. kontrola w oparciu o Greylist'y,
   j. białe i czarne listy definiowane globalnie oraz per użytkownik,
   k. weryfikacja źródłowego adresu IP,
   l. mechanizmy reputacji użytkownika,
   m. możliwe akcje dla poczty: Accept, Relay, Reject, Discard, Kwarnatanna, Oznaczanie (Tagging).
9. **Ochrona przed atakami DoS** – system musi zapewniać ochronę przed atakami typu:
   a. Denial of Service (Mail Bombing),
   b. ochrona przed atakami na adres odbiorcy,
   c. definiowanie maksymalnych ilości wiadomości pocztowych,
   d. kontrola Reverse DNS (Anty-Spoofing),
   e. weryfikacja poprawności adresu e-mail nadawcy.
10. **Parametry wydajnościowe i niezawodnościowe** – system musi zapewniać:
    a. ochronę minimum 2000 domen pocztowych,
    b. obsługę minimum 1700 lokalnych skrzynek pocztowych w trybie serwer,
    c. obsługę nie mniej niż 50 profili antywirusowych lub antyspamowych,
    d. skanowanie antyspamowe minimum 600 tys. wiadomości/godzinę.
11. **Bezpieczeństwo wiadomości** – system musi zapewniać:

a. mechanizmy szyfrowania wysyłanych wiadomości pocztowych, bez konieczności instalowania jakichkolwiek aplikacji na stacjach klienckich. Administrator powinien mieć możliwość włączenia tej funkcjonalności dla wybranych użytkowników,
b. wsparcie dla szyfrowanej komunikacji Gateway-to-Gateway,
c. wsparcie dla szyfrowanych protokołów: HTTPS, SMTPS, IMAPS, POP3S.

12. **Logowanie i raportowanie** – system musi zapewniać:
    a. możliwość definiowania polityki w oparciu w wbudowany kreator konfiguracji,
    b. logowanie SNMP dla zdarzeń systemowych z możliwością definiowania progów,
    c. logowanie do zewnętrznego serwera SYSLOG,
    d. logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych,
    e. powiadamianie o działalności wirusów,
    f. logowanie informacji na temat spamu oraz niedozwolonych załączników,
    g. predefiniowane szablony raportów,
    h. możliwość planowania czasu generowania raportów,
    i. możliwość podglądu logów w czasie rzeczywistym,
    j. archiwizacje poczty w oparciu o zestaw filtrów (np. słowa kluczowe).
13. **Tryb wysokiej dostępności (HA)** – system musi zapewniać:
    a. konfigurację klastra wysokiej dostępności w trybie Active-Passive w każdym z trybów: Gateway, transparent, serwer,
    b. tryb Active-Passive z synchronizacją polityk i wiadomości, gdzie klaster występuje pod jednym adresem IP,
    c. tryb synchronizacji konfiguracji dla scenariuszy rozległych (osobne adresy IP),
    d. wykrywanie awarii i powiadamianie administratora,
    e. monitorowanie stanu połączeń.
14. **Aktualizacje sygnatur, dostęp do bazy spamu** – system musi zapewniać:
    a. pracę w oparciu o bazę spamu uaktualnianą w czasie rzeczywistym,
    b. planowanie aktualizacji szczepionek antywirusowych w czasie (Scheduler),
    c. wymuszoną aktualizacja bazy wirusów (tryb push).
15. **Zarządzanie i raportowanie** – system musi zapewniać:
    a. lokalny interfejs zarządzania poprzez szyfrowane połączenie HTTPS, SSH,
    b. definiowanie wyglądu interfejsu zarządzania z możliwością wstawienia logo Zamawiającego.
16. **Serwisy i licencje:**
    a. Wykonawca musi dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres zobowiązania gwarancyjnego zawartego w ofercie Wykonawcy,
    b. Wykonawca musi zapewnić pierwszą linię wsparcia technicznego telefonicznie w języku polskim w trybie 8x5,

c. instalacja, konfiguracja oraz szkolenie z zakresu poprawnej i efektywnej eksploatacji systemu musi być przeprowadzone przez uprawnionego inżyniera Wykonawcy posiadającego certyfikat producenta zaoferowanego rozwiązania poświadczający znajomość instalacji i konfiguracji oferowanego systemu. Wykonawca musi zapewnić dostępność co najmniej dwóch inżynierów posiadających certyfikaty producenta oferowanego systemu.

17. **Certyfikaty** - dostarczony system powinien posiadać co najmniej poniższe certyfikaty:

    ICSA dla funkcjonalności Antyspam, VBSpam Platinium, Common Criteria EAL 2+, FIPS 140-2 Validation.

18. **Gwarancja**:

    a. system musi być objęty serwisem gwarancyjnym producenta przez okres co najmniej 24 miesiące (maksymalnie 36 miesięcy – zgodnie z zobowiązaniem zawartym w ofercie Wykonawcy), realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie systemu w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, Wykonawca przed podpisaniem umowy winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej,

    b. serwis powinien być realizowany przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta w zakresie serwisu gwarancyjnego (Wykonawca winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Polski), mających swoją siedzibę na terenie Polski. Zgłoszenia serwisowe przyjmowane w trybie 8x5 przez dedykowany serwisowy moduł internetowy,

    c. w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem zamówienia (tzw. produkty podwójnego zastosowania), Wykonawca winien przed podpisaniem umowy przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania,

    d. Wykonawca przed podpisaniem umowy winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

W zakres przedmiotu zamówienia wchodzi dostawa sytemu jego wdrożenie (instalacja i konfiguracja) w miejscu wskazanym przez Zamawiającego oraz warsztaty. Wykonawca takiej usługi jest zobowiązany do przedstawienia Zamawiającemu przed podpisaniem Umowy certyfikatów, wystawionych przed producenta oferowanego systemu, dla inżynierów przeprowadzających wdrożenie oraz warsztaty, które poświadczają zdanie egzaminów i znajomość konfiguracji dostarczonego systemu.

Wykonawca musi zorganizować zajęcia w formie jednodniowych (minimum 5 godzin zegarowych) warsztatów dla 20 wskazanych przez Zamawiającego użytkowników zaproponowanego przez Wykonawcę systemu, które będą integralną częścią wdrożenia. W trakcie warsztatów użytkownicy pod kierunkiem prowadzącego zdobędą umiejętności praktyczne potrzebne do prawidłowej i efektywnej eksploatacji systemu oraz wiedzy koniecznej do zapewnienia kompleksowego wsparcia użytkowników końcowych systemu.

Zakres wdrożenia będzie obejmował przynajmniej:

a. analizę konfiguracji obecnych polityk bezpieczeństwa na aktualnie użytkowanych przez Zamawiającego rozwiązaniach FortiWeb 400C (klaster), FortiGate 300C (klaster), FortiMail 200D (klaster w trybie Gateway) oraz FortiMail VM02 (w trybie serwer), wraz z aktualizacją firmware oraz optymalizacją zabezpieczeń zgodnie z najlepszymi praktykami oraz aktualnymi trendami panującymi w sferze zagrożeń dla chronionych systemów Zamawiającego (w szczególności poczty email),

b. przygotowanie środowiska (rejestracja i instalacja maszyny wirtualnej, aktualizacja oprogramowania),

c. konfiguracja systemu zgodnie z wymaganiami bezpieczeństwa organizacji (polityki, profile, moduły antyspam i antywirus, kwarantanna, szyfrowanie, archiwizacja),

d. weryfikacja poprawności implementacji (testy akceptacyjne),

e. kopia bezpieczeństwa konfiguracji wdrożonego systemu,

f. instruktarz obsługi systemu poprzez GUI.

Zakres tematyczny zagadnień które będą poruszane na warsztatach musi obejmować przynajmniej:

a. konfigurację środowiska,

b. konfigurację serwera, polityk routingu, konfigurację domen pocztowych, konfigurację profili antywirusowych/antyspamowych, konfigurację kalendarzy, zarządzanie użytkownikami, migrację skrzynek pocztowych, logi systemowe,

c. ochronę przed atakami DoS i Email Spoofing,

d. archiwizację i kwarantannę,

e. diagnostykę,

f. obsługę konta pocztowego, edycję danych własnych użytkownika, uruchamianie autorespondera, konfigurację stopki, zarządzanie katalogami, korzystanie z kalendarza.

Proponowana Agenda warsztatów:

godzina 10:00 – Rejestracja i przywitanie uczestników

godzina 10:30 – Rozpoczęcie ćwiczeń praktycznych

godzina 11:30 – Przerwa kawowa

godzina 11:45 – Kontynuacja ćwiczeń praktycznych

godzina 13:00 – Przerwa na obiad

godzina 13:45 – Kontynuacja ćwiczeń praktycznych

godzina 15:00 – Przerwa Kawowa

godzina 15:15 – Kontynuacja zajęć

godzina 16:45 – Koniec zajęć

Dla realizacji warsztatów Wykonawca zapewni:

- salę konferencyjną dostosowaną do przeprowadzenia warsztatów dla minimum 20 osób, wyposażoną w stoły, krzesła, projektor multimedialny, ekran lub białą ścianę do projekcji, flipchart z blokiem papierowym i pisakami, dostęp do Internetu. Sala konferencyjna powinna posiadać dobre oświetlenie, zaciemnienie oraz klimatyzację,
- przygotowanie techniczne sali konferencyjnej wraz z odpowiednim wyposażeniem oraz zapleczem technicznym umożliwiającym efektywne przeprowadzenie warsztatów,
- obsługę techniczną sprzętu, w tym sprawdzenie poprawności jego działania przed i w trakcie warsztatów, usuwanie usterek w trakcie trwania warsztatów,
- napoje gorące: kawę oraz herbatę (łącznie co najmniej 300ml na osobę) wraz z dodatkami mleko/śmietanka, cukier, cytryna,
- wodę gazowaną i niegazowaną (łącznie co najmniej 500ml na osobę),
- ciastka kruche/paluszki (co najmniej 80g na osobę),
- obiad składać się będzie się z: zupy w ilości co najmniej 300ml na osobę, dania głównego (co najmniej 2 rodzaje) oraz dwa dodatki skrobiowe (co najmniej 450-500g na osobę, w tym dodatek mięsny, rybny i jarski nie mniej niż 150g). Jako dodatek skrobiowy rozumie się ziemniaki, ryż, kaszę lub makaron, danie główne będzie obejmować potrawę mięsną, rybną i jarską. Dodatki do obiadu: sałaty i sałatki (łącznie co najmniej 100 g na osobę), kompot/sok (co najmniej 300ml na osobę),
- zaplecze gastronomiczne w którym serwowany będzie obiad musi znajdować się w odległości nie większej niż 500m w linii prostej od miejsca, w którym Wykonawca będzie realizował warsztaty.