

Opis przedmiotu zamówienia

Odnowienie wsparcia na system ochrony Poczty Elektronicznej

I. Skrótowy opis przedmiotu zamówienia:

- a. Przedmiotem zamówienia jest odnowienie świadczenia wsparcia przez Producentów na posiadany przez PGL LP system ochrony poczty elektronicznej bazujący na produktach Forcepoint Email Gateway oraz sandboxach Trellix Fireeye EX-3500 przez okres 36 miesięcy od daty zakończenia bieżących licencji.
- b. Świadczenie przez Wykonawcę usługi wsparcia do wymienionych w punkcie I.a. systemów przez okres 36 miesięcy od dnia podpisania umowy.

II. Szczegółowy opis przedmiotu zamówienia

1. Opis zakresu dostawy:

W ramach zamówienia Wykonawca dostarczy:

Odnowienie subskrypcji dla posiadanych przez PGL LP następujących składników systemu ochrony poczty elektronicznej:

1.1 Forcepoint Email Gateway składającego się z bramek pocztowych filtrujących ruch oraz centralnej konsoli zarządzającej dla 27 000 użytkowników na okres 36 miesięcy od daty wygaśnięcia aktualnego wsparcia tj. 28 lutego 2025r. Subskrypcja musi obejmować wszystkie posiadane aktualnie przez zamawiającego moduły oraz umożliwiać zgłaszania błędów producentowi, możliwość pobierania i instalacji patchy dla systemu oraz jego aktualizacji do najnowszych wersji.

1.2 Trellix składającego się z 6 urządzeń Trellix Fireeye EX3500 oraz centralnej konsoli zarządzającej na okres 36 miesięcy od daty wygaśnięcia aktualnego wsparcia tj. 12 lutego 2025r. Subskrypcja musi obejmować wszystkie posiadane aktualnie przez zamawiającego moduły oraz umożliwiać zgłaszania błędów producentowi, zdalny suport producenta, możliwość pobierania i instalacji patchy dla systemu, jego aktualizacji do najnowszych wersji oraz wymiany urządzeń na identyczne bądź lepsze w przypadku awarii.

2. **Opis usługi:** W ramach realizacji przedmiotu zamówienia Wykonawca będzie świadczył/realizował następujące usługi:

- 2.1. Wykonawca zapewni świadczenie usług wsparcia dla systemów Forcepoint Email Gateway oraz Trellix Fireeye EX-3500 przez okres 36 miesięcy od dnia podpisania umowy. Wsparcie Wykonawcy będzie świadczone zgodnie z następującymi zasadami:
- 2.1.1. Usługi wsparcia Wykonawcy będą świadczone w języku polskim.
 - 2.1.2. Awarie będą zgłaszane Wykonawcy przy pomocy kanału e-mail przez administratorów systemu ochrony poczty.
 - 2.1.3. Wykonawca ma prawo w imieniu zamawiającego rejestrować zgłoszenia suportowe w systemach producenta.
 - 2.1.4. Zamawiający będzie wykonywać zgłoszenia w dni robocze od poniedziałku do piątku w godzinach od 8:00 do 16:00. W przypadku zgłoszenia poza wyznaczonym oknem czasowym, przyjmuje się, że zostało ono zgłoszone z początkiem następnego dnia roboczego.
 - 2.1.5. Wykonawca w ciągu 2 godzin potwierdzi za pomocą kanału e-mail przyjęcie zgłoszenia.
 - 2.1.6. Awaria krytyczna zostanie usunięta w terminie do 12 godzin od godziny przesłania zgłoszenia. Awaria krytyczna rozumiana jest przez awarię systemu która uniemożliwia jego działanie lub działanie to drastycznie ogranicza. W szczególności zwiększa ryzyko utraty integralności, poufności danych i ich dostępności.[
 - 2.1.7. Awaria zwykła zostanie usunięta w terminie do 2 dni roboczych. Przez awarię zwykłą rozumiemy pozostałe awarie systemu.
 - 2.1.8. W przypadku gdy usunięcie Awarii będzie skutkować koniecznością wymiany zainstalowanego sprzętu Wykonawca w terminie do 14 dni roboczych od dnia zgłoszenia awarii na swój koszt dokona wymiany sprzętu na spełniający wymagania wskazane w OPZ tj. na sprzęt o tych samych lub lepszych parametrach. W ramach ww. wymiany Wykonawca wykona instalację urządzenia.
W przypadku gdy ww. wymiana sprzętu dotyczy awarii krytycznej skutkującej niemożliwością przekazywania wiadomości e-mail, jeżeli nie jest możliwa wymiana urządzenia w przeciągu 12 godzin, Wykonawca dostarczy w tym czasie urządzenie zastępcze do czasu dostarczenia urządzenia sprawnego.

III. Opis rozwiązania równoważnego - kryteria stosowane w celu oceny równoważności:

1. Rozwiązanie równoważne dla systemu ochrony poczty musi spełniać następujące wymagania:

Wymagania ogólne:

- 1 Dla zapewnienia wysokiej sprawności i skuteczności działania wszystkie elementy Rozwiązania muszą pracować w oparciu o dedykowany system operacyjny producenta. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych ogólnego przeznaczenia na których zainstalowano aplikacje realizujące wymagane funkcje
- 2 Zamawiający oczekuje dostawy Rozwiązania ochrony poczty elektronicznej, które będzie realizować następujące funkcje:
 - 2.1 ochronę przed szkodliwą treścią (m.in. malware, wirusy etc.)
 - 2.2 ochronę przed spamem
 - 2.3 filtrowanie treści przesyłanej w poczcie elektronicznej (w tym załączniki)
 - 2.4 ochronę przez niebezpiecznymi linkami URL w treści wiadomości
 - 2.5 rozwiązanie musi umożliwiać kontrolę protokołu SMTP w tym szyfrowane wersje tego protokołu: SSL i TLS.
 - 2.6 rozwiązanie musi zapewniać filtrowanie poczty przychodzącej i wychodzącej (w tym poczty wewnętrznej), przy czym musi istnieć możliwość przypisania odrębnych polityk dla każdego z kierunków przesyłania poczty elektronicznej.
 - 2.7 Rozwiązanie musi zapewniać ochronę dla komunikacji z wykorzystaniem protokołu IPv4 oraz IPv6
 - 2.8 Zamawiający nie wymaga aby całość rozwiązania pochodziła od jednego producenta.
- 3 Rozwiązanie musi pracować jako gateway dla poczty elektronicznej (jako MTA - Mail Transfer Agent). Dla ochrony poczty wewnętrznej (internal), której ruch nie przechodzi przez gateway a zamyka się wewnątrz farmy serwerów pocztowych, wymagane jest zastosowanie mechanizmu chroniącego pocztę bezpośrednio na serwerach Exchange.
- 4 Wymagania logowania Rozwiązania
 - 4.1 rozwiązanie powinno pozwalać na przeszukiwanie wiadomości email z wykorzystaniem parametrów minimum:
 - 4.1.1 Nadawca
 - 4.1.2 Odbiorca
 - 4.1.3 Temat
 - 4.1.4 Czas dostarczenia
 - 4.1.5 Nazwa serwera
 - 4.1.6 IP nadawcy
 - 4.1.7 Załącznik
 - 4.1.8 Nagłówek Message-ID
 - 4.1.9 Sumie kontrolnej załącznika (min. MD5 i SHA256)
- 5 Rozwiązanie powinno umożliwiać informowanie za pomocą protokołu SNMP o zdarzeniach generowanych przez system wymagających uwagi administratora.
- 6 Rozwiązanie powinno logować informacje o krytycznych zdarzeniach

systemowych.

- 7 Rozwiązanie powinno zawierać predefiniowane szablony raportów
- 8 Rozwiązanie musi umożliwiać automatyczne wykonywanie kopii zapasowej konfiguracji zgodnie z harmonogramem lub w sposób manualny.
- 9 Rozwiązanie musi obsłużyć ruchu na poziomie szczytowym minimum 40tys. wiadomości na godzinę przychodzących z Internetu oraz 12 tys. wiadomości na godzinę wysyłanych z serwerów Exchange do Internetu

Architektura dla kompletnego Rozwiązania:

- 10 Rozwiązanie musi składać się z urządzeń pracujących w trybie MTA (Relay pocztowy), z możliwością wykrywania i blokowania zagrożeń.
- 11 Jeżeli Rozwiązanie zawierać będzie maszyny wirtualne muszą one być możliwe do uruchomienia na platformie VMware.
- 12 Rozwiązanie musi być dedykowanym MTA (Mail Transfer Agent) pracującym w trybie bramy dla ruchu przychodzącego i wychodzącego.
- 13 Rozwiązanie musi być wdrożone w trybie wysokiej dostępności (bez dodatkowych licencji wymaganych do uruchomienia tych funkcjonalności) poprzez dostarczenie i zastosowanie jednego z rozwiązań:
 - 13.1 Redundancja każdego elementu systemu w obu centrach przetwarzania Lasów Państwowych (active-active z rozkładem obciążenia. Rozkład obciążenia może być realizowany z wykorzystaniem konfiguracji DNS i rekordów MX).
 - 13.2 Zastosowanie konfiguracji mieszanej z wykorzystaniem mechanizmów wirtualizatora i mechanizmów układu Active-Pasive oraz mechanizmów w układzie failover
 - 13.3 Zastosowanie konfiguracji Active-Passive, z synchronizacją danych na poziomie klastrów/węzłów.
- 14 Rozwiązanie musi wspierać protokoły SMTP, ESMTP, Secure SMTP over TLS.
- 15 Systemy operacyjne rozwiązania muszą posiadać specjalnie zaprojektowany mechanizm do obsługi I/O, zoptymalizowany do obsługi poczty elektronicznej.
- 16 Konfiguracja urządzenia musi być możliwa przez:
 - 16.1 Interfejs Web: HTTPS
 - 16.2 CLI: przez SSH
- 17 Urządzenia muszą wspierać następujące mechanizmy kryptograficzne:
 - 17.1 TLS: TLS w wersji przynajmniej 1.2 z możliwością zablokowania użycia starszych wersji protokołu
 - 17.2 DomainKeys Signing: 512-, 768-, 1024-, 1536- i 2048-bit RSA
- 18 Kwarantanna poczty z podsumowaniem (Digest). Wiadomość wysyłana jako Digest do odbiorcy musi posiadać możliwość minimum:
 - 18.1 Wysyłki zgodnie z harmonogramem: dziennym, tygodniowym
 - 18.2 Lokalizacji językowej (pełne wsparcie dla języka polskiego w tym opisy przycisków. Dopuszczone jest rozwiązanie posiadające możliwość personalizacji nagłówków/treści w j. polskim, zachowując niektóre elementy wiadomości/strony w j. angielskim).
- 19 Dostęp do kwarantanny przez portal www (SSL) z autentykacją AD. Portal www dla użytkownika musi posiadać możliwości dopasowania do użytkownika takie jak:
 - 19.1 Modyfikacja akcji typu zwolnij/usuń/zaraportuj false-positives/odczytaj dla

- odpowiednich folderów widocznych w portalu kwarantanny użytkownika.
- 19.2 Zamawiający dopuści rozwiązanie posiadające stały podział folderów kwarantanny według typu na spam, antywirus, wiadomości z plikami poddanymi analizie, wiadomości skierowane przez polityki, wiadomości niesklasyfikowane
- 20 Możliwość kwarantannowania w celach audytowych wiadomości, które zostały skategoryzowane jako bezpieczne.
- 21 Rozwiązanie musi zapewniać możliwość definiowania list zaufanych i blokowanych nadawców.
- 22 Rozwiązanie musi umożliwiać definiowanie i przeglądanie katalogów kwarantanny dla różnych reguł antywirusowych i antyspamowych.

Definiowanie polityk:

- 23 Polityki filtrowania tworzone w oparciu o parametry takie jak:
- 23.1 adres e-mail nadawcy/odbiorcy
 - 23.2 nazwy użytkownika/grupy LDAP
 - 23.3 adresy IP
 - 23.4 nagłówki wiadomości przychodzących/wychodzących
 - 23.5 wielkość załącznika
 - 23.6 rozszerzenie (rodzaj) załączników
- 24 Rozwiązanie musi umożliwiać definiowanie co najmniej następujących akcji (w ramach polityki):
- 24.1 dostarczenie wiadomości z wykonaniem dodatkowych akcji:
 - 24.2 zmodyfikowanie tematu przesyłki
 - 24.3 usunięcie i/lub dodanie nagłówka X-header
 - 24.4 wysłanie kopii wiadomości pod wskazany adres lub adresy email
 - 24.5 zablokowanie wiadomości
 - 24.6 zapisanie wiadomości do wskazanego folderu kwarantanny
 - 24.7 wysłanie powiadomienia w tym (odbiorcy, nadawcy, adresu trzeciego)
- 25 Rozwiązanie musi umożliwiać budowanie polityk i wyjątków od polityk, obejmujących wszystkie funkcjonalności produktu, niezależnie dla ruchu wychodzącego i przychodzącego z zastosowaniem co najmniej:
- 25.1 domen email
 - 25.2 adresów pojedynczych nadawców/odbiorców
- 26 Rozwiązanie musi umożliwiać tworzenie odrębnych polityk i wyjątków dla różnych grup użytkowników.
- 27 Rozwiązanie musi umożliwiać tworzenie dedykowanych polityk dla tzw. „greymail” (wiadomości, które nie są kwalifikowane jako spam); dla takich wiadomości musi istnieć możliwość ich jednoznacznego znakowania.

Realizacja ochrony antyspamowej:

- 28 Rozwiązanie powinno posiadać rozbudowane narzędzia zapobiegania przesyłaniu SPAM do serwera pocztowego. W tym celu system musi zapewniać mechanizmy ochrony oparte co najmniej o:
- 28.1 Sygnatury
 - 28.2 Słowniki
 - 28.3 Heurystykę, dla której musi być możliwa regulacja czułości (kontrola ilości False-Positives)

- 29 Rozwiązanie musi posiadać wbudowane mechanizmy metody wykrywania wiadomości komercyjnych typu „Newsletters” i umożliwiać traktowanie tych wiadomości w zależności od ustalonej polityki organizacji jako SPAM lub jako wiadomość dopuszczona
- 30 Rozwiązanie musi zapewnić opcję definiowania wyjątków od stosowanych polityk
- 31 Mechanizm antyspamowy musi być realizowany wielofazowo w oparciu o reputację IP oraz reputację nadawcy)
 - 31.1 Heurystyczna analiza spamu.
 - 31.2 Filtrowanie treści załączników (analiza kontekstowa).
 - 31.3 Szczegółowa kontrola nagłówka wiadomości.
 - 31.4 Analiza poczty w oparciu o dynamiczną bazę spamu dostarczaną przez tego samego producenta.
 - 31.5 Białe i czarne listy definiowane globalnie
 - 31.6 Kwarantanna oraz oznaczanie spamu. Kwarantanna znajduje się na serwerze zarządzającym (brak potrzeby instalacji dodatkowego serwera kwarantanny).
- 32 Rozwiązanie musi weryfikować reputację adresów IP w ogólnodostępnej bazie reputacji.
- 33 Reguły muszą weryfikować informację na temat adresów IP pojawiających się w mailach jako linki do stron, strukturę wiadomości, sposób w jaki została wysłana, treść wiadomości i reputację nadawcy.
- 34 Reguły powinny być uaktualniane, automatycznie, nie rzadziej niż co 15 minut przez sieć Internet.
- 35 Rozwiązanie musi posiadać możliwość skorzystania z funkcji reverse DNS lookup do określenia nazwy domeny dla adresu IP nadawcy wiadomości przychodzącej, wykonanie weryfikacji oraz odrzucenie połączenia w przypadku:
 - 35.1 braku rekordu PTR w DNS
 - 35.2 niezgodności nazwy domeny przesłanej w komunikacie SMTP HELO/EHLO z nazwą domeny w rekordzie DNS,
 - 35.3 niezgodności rekordu reverse DNS (PTR) z rekordem forward DNS (A)
- 36 Rozwiązanie musi umożliwiać weryfikację nadawcy wiadomości w oparciu o mechanizm SPF (Sender Policy Framework). Rozwiązanie powinno umożliwiać co najmniej:
 - 36.1 odrzucenie lub przyjęcie wiadomości, jeżeli rekord SPF nie istnieje
 - 36.2 odrzucenie wiadomości, jeżeli rekord SPF nie pasuje do domeny nadawcy
- 37 Ochrona przed atakami DoS – System musi posiadać:
 - 37.1 Denial of Service (Mail Bombing).
 - 37.2 Ochrona przed atakami na adres odbiorcy.
 - 37.3 Definiowanie maksymalnych ilości wiadomości pocztowych.
 - 37.4 Kontrola Reverse DNS (Anty-Spoofing).
 - 37.5 Weryfikacja poprawności adresu e-mail nadawcy.
- 38 Rozwiązanie musi umożliwiać:
 - 38.1 monitorowanie i ograniczanie ilości połączeń z jednego adresu IP w określonym przedziale czasu.
 - 38.2 musi zapewniać opcję ograniczenia jednoczesnych aktywnych połączeń
 - 38.3 musi zapewniać opcję ograniczenia maksymalnej ilości połączeń i wiadomości.
 - 38.4 ograniczanie maksymalnej liczby wiadomości przekazywanych za pomocą pojedynczego połączenia SMTP

39 Rozwiązanie musi posiadać możliwość filtracji plików za pomocą mechanizmów takich jak:

- 39.1 Wielkość załącznika.
- 39.2 Rozszerzenie pliku.
- 39.3 Nazwa pliku.
- 39.4 Type MIME.

40 Rozwiązanie musi pozwalać na blokowanie na określony czas przyjmowania poczty z adresów IP, dla których odnotowano wiadomości zawierające zdefiniowaną liczbę niewłaściwych adresatów z chronionej domeny lub ograniczyć liczbę połączeń.

Ochrona Antywirusowa:

41 Rozwiązanie musi zapewniać blokowanie złośliwej treści:

- 41.1 z wykorzystaniem tradycyjnego skanowania antywirusowego opartego o komercyjny silnik antywirusowy oraz bazę sygnatur kodów złośliwych
- 41.2 z wykorzystaniem zaawansowanych technik wykrywania zagrożeń jak metody oparte o heurystykę i analizy w czasie rzeczywistym
- 41.3 musi zapewniać możliwość blokowania niebezpiecznych treści typu ActiveX, Javascript lub VB script.

42 Rozwiązanie musi umożliwiać definiowanie wyjątków od stosowanych polityk,

43 Rozwiązanie musi mieć możliwość wyboru z co najmniej dwóch komercyjnych silników antywirusowych (na jednej platformie sprzętowej) lub za pomocą dodatkowego urządzenia.

44 Silnik antywirusowy musi korzystać z następujących metod skanowania wiadomości:

- 44.1 dopasowanie wzorców binarnych do sygnatur antywirusowych
- 44.2 analiza heurystyczna
- 44.3 emulacja uruchomienia kodu (w celu zapobiegania infekcji wirusami polimorficznymi)

45 Mechanizm musi mieć do dyspozycji oddzielną od dedykowanej dla spamu, kwarantannę, do której dostęp ma tylko administrator.

46 Rozwiązanie musi zapewniać mechanizmy ochrony przed epidemią złośliwego kodu.

47 mechanizm antywirusowy musi posiadać technologię umożliwiającą automatyczną kwarantannę wiadomości, które pomimo, że nie są wskazane przez powyższe metody skanowania (z powodu np. braku odpowiednich sygnatur antywirusowych), mogą jednak zawierać złośliwy kod.

47.1 informacje o takim podejrzeniu powinny być wysyłane przed globalną bazę reputacji, o parametrach opisanych w wymogach modułu antyspamowego.

Filtrowanie i kontrola treści:

48 Rozwiązanie musi umożliwiać filtrowanie i kontrolę treści

49 Kontrola treści wiadomości co najmniej w zakresie:

- 49.1 słowa kluczowe
- 49.2 słowniki
- 49.3 wyrażenia regularne
- 49.4 typ załączników

- 50 Kontrola musi obejmować co najmniej następujące elementy wiadomości:
- 50.1 tytuł,
 - 50.2 treść,
 - 50.3 nagłówki,
 - 50.4 adres nadawcy
 - 50.5 adres odbiorcy
- 51 Proponowane rozwiązanie musi posiadać mechanizmy analizy i filtrowania oraz zarządzania treścią wiadomości poczty elektronicznej, zarówno treści samej wiadomości jak i jej załączników.
- 52 Rozwiązanie musi zapewniać wsparcie dla standardu Domain-based Message Authentication Reporting & Conformance (DMARC).
- 53 Rozwiązanie musi zapewniać wsparcie dla standardu Sender Policy Framework (SPF).
- 54 Rozwiązanie musi zapewniać wsparcie dla standardu Domain Keys Identified Mail (DKIM).
- 55 Rozwiązanie musi umożliwiać zarządzanie kwarantanną (folderami) dla blokowanych wiadomości w zakresie zarządzania predefiniowanymi oraz tworzenia nowych.
- 56 Rozwiązanie powinno zawierać moduł umożliwiający identyfikację chronionych informacji z użyciem mechanizmów
- 56.1 słowa kluczowe
 - 56.2 słowniki
 - 56.3 wyrażenia regularne
 - 56.4 właściwości przesyłanych plików takie jak prawdziwy typ pliku, jego nazwa lub rozmiar
- 57 Rozwiązanie musi zapewniać kwarantannę dla zablokowanych wiadomości. Dla kolejki kwarantanny musi być możliwe zdefiniowanie jej maksymalnej wielkości oraz czasu, po którym wiadomości będą usuwane.

Kryptografia i szyfrowanie:

- 58 Rozwiązanie musi posiadać mechanizmy oznaczania poczty wychodzącej (Bounce Address Tag Validation (BATV)) oraz weryfikacji tego oznaczenia w przypadku otrzymania wiadomości odbitej od odbiorcy (tzw. Bounce) w celu ochrony przed atakami typu „misdirected bounce spam”
- 59 Rozwiązanie musi obsługiwać standard DKIM (Domain Keys Identified Messages) używany w celu uwierzytelnienia poczty, za pomocą szyfrowania asymetrycznego.
- 60 Rozwiązanie musi umożliwiać opcjonalnie, oddzielnie licencjonowane, szyfrowanie symetryczne poczty dla wybranych wiadomości, wykonywane bez potrzeby jakiegokolwiek ingerencji w klienta pocztowego oraz bez potrzeby implementacji PKI.
- 61 Rozbudowa o funkcje kryptografii i uwierzytelnienia musi się wiązać co najwyżej z wykupieniem odpowiedniej licencji u producenta rozwiązania i jej imporcie w systemie.

Moduł raportujący i zarządzający:

- 62 Każdy komponent Rozwiązania musi posiadać wbudowany moduł zarządzający

i raportujący.

63 Rozwiązanie musi być wyposażone w system raportujący, umożliwiający:

63.1 generowanie predefiniowanych raportów na żądanie oraz zgodnie z harmonogramem.

63.2 system powinien umożliwiać generowanie raportów codziennych, tygodniowych oraz miesięcznych.

63.3 powinno być możliwe dostarczanie raportów w postaci plików pdf, html lub csv.

63.4 powinno być możliwe dostosowanie tematu i treści automatycznie wysyłanego maila zawierającego generowane raporty.

64 Zarządzanie, przeglądanie aktywności użytkowników oraz raportowanie powinny być dostępne z webowej konsoli administracyjnej.

65 Dostęp do webowej konsoli zarządzającej powinien odbywać się w bezpiecznym połączeniu HTTPS.

66 Konsola zarządzająca powinna zawierać ekran przedstawiający wykres sumarycznej aktywności z ostatnich 24 godzin oraz podstawowe statystyki.

67 Rozwiązanie powinien udostępniać mechanizm pozwalający na przeglądanie przez chronionych użytkowników wiadomości umieszczonych w kwarantannie, umożliwiając im również zwolnienie wybranych wiadomości z kwarantanny

Wymagania sprzętowe - instancja wirtualna:

68 Rozwiązanie musi być dedykowanym MTA (Mail Transfer Agent) pracującym w trybie bramy dla ruchu przychodzącego i wychodzącego.

69 Rozwiązanie powinno być zrealizowane w postaci dostawy urządzeń fizycznych lub instancji wirtualnych systemu VMware eliminując dodatkowy koszt Zamawiającego związany z zakupem sprzętu.

70 Licencje na bramki przyjmujące pocztę powinny posiadać opcję skalowania w celu uzyskania większej wydajności na kolejne maszyny wirtualne w środowisku wirtualnym będącym w posiadaniu Zamawiającego bez ponoszenia dodatkowych kosztów.

71 Proponowane rozwiązanie powinno być posadowione na redundantnych maszynach pracujących w trybie aktywny-aktywny bez dodatkowych licencji wymaganych do uruchomienia tych funkcjonalności. Wymagane jest zastosowanie odpowiedniej nadmiarowości modułów Rozwiązania aby w przypadku awarii jednego z centrum danych utrzymać wymaganą wydajność i pełną funkcjonalność.

72 Systemy operacyjne muszą posiadać specjalnie zaprojektowany mechanizm do obsługi I/O, zoptymalizowany do obsługi poczty elektronicznej.

73 Rozwiązanie powinno być przygotowane do pełnej obsługi 27 000 tysięcy użytkowników, nawet w przypadku awarii całkowitej i nieosiągalności jednego z centrum danych.

Wymagane licencje:

74 Proponowane rozwiązanie musi być zaoferowane z możliwością instalacji systemu na nieograniczonej liczbie maszyn wirtualnych

75 Proponowane rozwiązanie powinno posiadać licencje dla ochrony 27 000 tysięcy skrzynek pocztowych ze wsparciem producenta na okres 36 miesięcy (z

możliwością przedłużenia).

- 76 Każdy komponent Rozwiązania musi zostać dostarczony ze scentralizowaną konsolą zarządzającą umożliwiającą wspólne zarządzanie politykami i raportowanie

Wymagania Rozwiązania zaawansowanej ochrony antymalware:

- 77 Rozwiązanie musi posiadać mechanizmy zaawansowanej ochrony antymalware
- 78 Mechanizmy zaawansowanej ochrony antymalware muszą obejmować:
- 78.1 sprawdzenie reputacyjne dla plików przesyłanych przez urządzenie
 - 78.2 monitorowanie wsteczne dla plików już przesłanych przez minimum 30 dni, a informacje o tym przetrzymywane przez minimum 180 dni.
- 79 W przypadku zatrzymania podejrzanej wiadomości administrator musi mieć możliwość podejrzenia wiadomości w trybie surowym (pełna wiadomość w wersji tekstowej ze wszystkimi nagłówkami) oraz w wersji sformatowanej z interpretacją kodu HTML (w czytelnym trybie użytkownika)
- 80 Kontrola reputacji dla plików i adresów URL musi odbywać się w ogólnodostępnej bazie reputacji
- 81 Kontrola reputacji musi odbywać się na podstawie unikalnych metadanych własnościowych pliku, nie jest dopuszczalne, aby sprawdzenie reputacyjne wymuszało przesłanie pliku na zewnątrz systemu kontroli poczty.
- 82 Funkcja sandboxingu dla plików przesyłanych pocztą elektroniczną musi być wbudowana w system ochrony poczty w postaci dedykowanych urządzeń zintegrowanych z systemem poczty elektronicznej. Nie jest dopuszczalne stosowanie zewnętrznych systemów firm trzecich.
- 83 Analiza statyczna i dynamiczna muszą się odbywać w na dostarczonych urządzeniach – nie jest dopuszczalne wysyłanie plików do analizy poza siedzibę Zamawiającego.
- 84 Rozwiązanie powinno umożliwiać uruchomienie nie mniej niż 56 maszyn wirtualnych wykonujących analizę jednocześnie. Zamawiający poprzez liczbę 56 określa ilość dostępnych maszyn wirtualnych, która ma być dostępna do analizy nawet w przypadku awarii jednego z urządzeń analizujących.
- 85 Analiza dynamiczna powinna wykorzystywać dedykowane środowisko wirtualne (hypervisor),
- 86 Środowisko, w którym jest wykonywana analiza dynamiczna, musi posiadać mechanizmy utrudniające jego wykrycie przez analizowany malware.
- 87 Maszyny wirtualne, w których wykonywana jest analiza zachowania ataku, muszą posiadać mechanizmy symulacji realnego użytkownika (w tym co najmniej: ruchy i kliknięcia myszą, historię odwiedzanych stron web, historię otwieranych dokumentów)
- 88 Funkcja monitorowania wstecznego musi umożliwiać informowanie administratora o zmianie decyzji dotyczących plików uprzednio przesłanych przez urządzenie. W szczególności dotyczy to sytuacji, gdy we wskazanym pliku wykryto złośliwy kod.
- 89 Funkcja monitorowania wstecznego musi umożliwiać informowanie administratora o zmianie decyzji dotyczących URL uprzednio analizowanego przez urządzenie. W szczególności dotyczy to sytuacji, gdy we wskazanym URL wykryto zagrożenie. (Zamawiający dopuści rozwiązanie, w którym wiadomości zawierające nie skategoryzowane URL będą przenoszone do tymczasowej

- kwarantanny i ew. zwalniane lub blokowane po uzyskaniu werdyktu z centrum analitycznego producenta rozwiązania).
- 90 Analiza dynamiczna musi być wykonywana z wykorzystaniem różnych wersji systemów operacyjnych Microsoft Windows (przynajmniej Windows 7 oraz Windows 10), i przynajmniej jednej wersji systemu Linux oraz różnych aplikacji i różnych ich wersji (co najmniej FireFox, Chrome, IE, Adobe Reader, Java JDK JRE, MS Office, RunDLL)
- 91 Analiza dynamiczna musi się odbywać z wykorzystaniem osobnego interfejsu poprzez dedykowaną linię do Internetu (brudne łącze) zapewnione przez Wykonawcę. Połączenie posiada własną adresację IP, default gateway i serwer DNS.
- 92 Rozwiązanie musi analizować co najmniej następujące rodzaje plików: (Rozszerzenia używane przez pakiet OFFICE-np. DOC/DOCX, XLS/XLSX, PPT/PPTX , oraz EXE, DLL, CHM, RAR, ACE, SCR, PDF, PUB, ZIP, MP3, 7Z, BZ, GZ, JAR, MHT, RTF, CAB
- 93 Zamawiający nie może ponosić dodatkowych kosztów związanych z licencjami OS i aplikacji używanymi w maszynach wirtualnych oraz kosztów ich aktualizacji. (muszą zostać dostarczone przez producenta w ramach Rozwiązania)
- 94 Analiza ataku musi umożliwiać wykrywanie zagrożeń typu kernel rootkit, code injection, DLL injection, heap spraying.
- 95 W wyniku analizy Rozwiązanie musi zapewniać dostęp do szczegółowych danych analitycznych (forensic data) z przeprowadzonej analizy, w tym co najmniej:
- 95.1 adresy URL jeśli są związane z analizowanym malware,
 - 95.2 funkcje skrótu (hash)
 - 95.3 wykryty plik malware
 - 95.4 sekwencyjny (od startu podejrzanego kodu do zakończenia analizy) zapis zmian wykonywanych przez malware w maszynie wirtualnej, która przeprowadzała analizę: zmiany w systemie operacyjnym, rejestrze, systemie plików, sposobie startu systemu, informacja o próbach nawiązania połączenia sieciowego przez malware wraz z plikami PCAP z nagraniem takich prób
- 96 Rozwiązanie musi zwrócić po każdej analizie dynamicznej, w której wykryto niebezpieczny kod lub inne zagrożenie, zestaw artefaktów jakie zostały utworzone, pobrane czy zmodyfikowane wewnątrz maszyny wirtualnej; przynajmniej pobierane i uruchamiane plik wykonywalne, zmiany w rejestrze, tworzone pliki.
- 97 Rozwiązanie musi umożliwiać otwieranie i analizowane zaszyfrowanych archiwów przesyłanych w wiadomościach poczty elektronicznej przy założeniu, że hasło do archiwum jest przesyłane w treści wiadomości.
- 98 Powinno być możliwe dodawanie własnych słów kluczowych oraz haseł, używanych następnie przez urządzenie do dekompresji zaszyfrowanych załączników. (Zamawiający dopuści system nie posiadający takich funkcjonalności, pozwalający przy tym na blokowanie wiadomości z szyfrowanymi załącznikami)

Analiza adresów URL:

- 99 System antymalware musi wykonywać głęboką analizę adresów URL po stronie Zamawiającego realizując:
- 99.1 Wykrywanie phishingu poprzez analizę zawartości strony WEB na którą kieruję URL w wiadomości email.
 - 99.2 Analiza antyphishing obejmować musi treść strony, pliki graficzne, pola formularzy w celu wykrywania podobieństw do prawdziwych serwisów
 - 99.3 W przypadku wykrycia phishing system musi wykonać zrzut (screen) niebezpiecznej strony web w celu dostarczenia administratorowi i/lub użytkownikowi dodatkowych informacji i umożliwić potwierdzenie alertu
- 100 Funkcjonalność analizy URL musi obsługiwać skrócone adresy URL (z tzw. serwisów shortener URL), co najmniej dla następujących serwisów: bit.ly, t.co, goo.gl,youtu.be, ow.ly, tiny.cc, tinyurl.com, fb.me, ibm.bz, apple.co, conta.cc, j.mp, urlcut.org, xurl.es, a1.to, bit.do, lnkd.in, db.tt, qr.ae, adf.ly, cur.lv. Zamawiający dopuszcza alternatywnie serwisy tumblr.com, ff.im, tl.gd, plurk.com, url4.eu, yfrog.com, alturl.com, wp.me, chatter.com, ur.ly oraz obsługujące do 10 poziomów zagnieżdżenia skrótów.
- 101 Rozwiązanie musi umożliwiać włączenie lub wyłączenie funkcji nadpisywania podejrzanych adresów URL o nieznanej reputacji, wykrytych w treści wiadomości – przed jej dostarczeniem do odbiorcy – celem przekierowania połączenia w momencie kliknięcia podejrzanego URL i wykonania ponownej analizy.
- 102 W przypadku wykrycia zagrożenia w przepisany URL, użytkownik końcowy po kliknięciu URL, powinien być przekierowywany do strony informującej (w języku polskim) o zablokowaniu takiej komunikacji pomimo że cała wiadomość została dostarczona. Dopuszczalne jest zaoferowanie systemu posiadającego możliwość personalizacji nagłówków/treści w j. polskim, zachowując niektóre elementy wiadomości/strony w j. angielskim
- 103 W przypadku tylko podejrzenia zainfekowania danego URL bez potwierdzenia zagrożenia, użytkownik końcowy po jego kliknięciu, powinien być informowany o ograniczonym zaufaniu do takiej witryny i powinno być możliwe przejście na stronę wskazaną przez URL (w języku polskim). Dopuszczalne jest zaoferowanie systemu posiadającego możliwość personalizacji nagłówków/treści w j. polskim, zachowując niektóre elementy wiadomości/strony w j. angielskim. W innych przypadkach użytkownik końcowy, po jego kliknięciu powinien być automatycznie przenoszony do oryginalnej lokalizacji adresu.

Wymagania sprzętowe:

1. Dostarczone urządzenia muszą być fabrycznie nowe i nieużywane, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia oraz wolne od wad fizycznych i prawnych, ponadto muszą być objęte gwarancją i wsparciem technicznym producenta obowiązującym od dnia zgłoszenia do odbioru dostawy sprzętu do końca okresu obowiązywania umowy, świadczoną przez organizację serwisową producenta, mającego swoją placówkę serwisową na terenie Polski.
2. Oferowane modele muszą znajdować się w sprzedaży, co najmniej od 30 dni poprzedzających termin złożenia oferty.

3. Wszystkie oferowane urządzenia muszą być wyprodukowane zgodnie z normą jakości ISO 9001:2000 lub normą równoważną.
4. Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
5. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
6. Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230V/400V \pm 10%, Obowiązkiem Wykonawcy jest uzupełnienie brakujących elementów systemu zasilania zgodnie z wymaganiami oferowanych urządzeń.
7. Każde urządzenie, wyposażone w przyłączy do sieci energetycznej musi mieć zainstalowane wszystkie przewidziane przez producenta układy zasilające i chłodzące.
8. Dostarczone urządzenia muszą umożliwiać instalację w standardowych szafach montażowych 19", o głębokości 90 cm. Wysokość zajętej przestrzeni nie może przekraczać łącznie wysokości 8U w każdej z lokalizacji. Wyższa przestrzeń wymaga konsultacji i akceptacji Zamawiającego.

2. W przypadku zaoferowania rozwiązania równoważnego Wykonawca przygotowuje i dostarczy w przeciągu 5 dni roboczych od dnia podpisania umowy na swój koszt do siedziby Zamawiającego środowisko testowe na podstawie którego zostanie sprawdzone spełnienie wymagań OPZ.
3. W przypadku akceptacji rozwiązania równoważnego Wykonawca przygotowuje w terminie 10 dni roboczych od dnia akceptacji przez Zamawiającego rozwiązania o którym mowa w pkt.2 dokumentację przedwdrożeniową obejmującą:
 - Nazwy i ilości sprzętu oraz oprogramowania jakie zostanie dostarczone
 - opis konfiguracji rozwiązania
 - architekturę sieciową rozwiązania z uwzględnieniem infrastruktury PGL LP.
 - diagramy przepływu wiadomości
 - konfiguracje poszczególnych elementów systemu
4. W terminie do 7 dni roboczych od akceptacji dokumentacji przedwdrożeniowej Wykonawca, który zaoferował rozwiązanie równoważne przeprowadzi na swój koszt wdrożenie tego rozwiązania. W ramach wdrożenia zmigruje wszystkie dane z obecnego systemu ochrony poczty do rozwiązania równoważnego włączając w to wszelkie białe i czarne listy, reguły przetwarzania wiadomości, wszystkie wiadomości w kwarantannach systemowych i użytkowników.

5. W przeciągu 7 dni roboczych od dnia odbioru wdrożenia zostanie dostarczona dokumentacja powdrożeniowa obejmująca zakresem elementy dokumentacji przedwdrożeniowej oraz dodatkowo:
 - wykaz zmian w stosunku do dokumentacji przedwdrożeniowej
 - wykaz sprzętu
 - wykaz licencji / subskrypcji / oprogramowania
 - wykaz wszystkich czynności dokonanych podczas wdrożenia
 - opis (w postaci procedur lub instrukcji) wszystkich rutynowych czynności administracyjnych dla wdrożonego rozwiązania jak również działań pozwalających na utrzymanie wymaganej dostępności, wydajności, bezpieczeństwa wdrożonego rozwiązania.
 - opis zasad konserwacji i utrzymania systemu tj. informacja o okresowych zadaniach, które muszą być wykonane przez Zamawiającego, np.: weryfikacja zajętości przestrzeni, konieczność wykonywania analizy tabel, czyszczenia logów (dobre praktyki administracyjne).
 - procedury backupu i odtwarzania
 - procedury aktualizacji
6. Wykonawca, który zaoferował rozwiązanie równoważne przed zakończeniem etapu wdrożenia przeprowadzi na swój koszt szkolenie stacjonarne dla 5 administratorów Zamawiającego. Zakres szkolenia obejmie administrację rozwiązaniem równoważnym. Szkolenie zostanie przeprowadzone przez certyfikowanego we wdrażanym rozwiązaniu Instruktora. Czas szkolenia minimum 16 godzin w ośrodku szkoleniowym na terenie Warszawy lub okolic (do 25km).
7. W okresie wdrażania systemu równoważnego Wykonawca musi zapewnić ochronę poczty elektronicznej PGL LP.