**Załącznik nr 2 do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**CZĘŚĆ 1 -OPROGRAMOWANIE**

# **System uwierzytelniania, autoryzacji i kontroli dostępu**

Oferowane rozwiązanie musi pozwalać na centralne zarządzenie kontami użytkowników oraz procesem uwierzytelnienia – w tym celu musi zapewniać wszystkie wymienione poniżej funkcje.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne, odpowiednio zabezpieczone systemy operacyjne dla poszczególnych komponentów.

|  |  |  |
| --- | --- | --- |
| L.P |  | PROSZĘ WPISAĆ CZY OFEROWANY PRZEDMIOT ZAMÓWIENIA**SPEŁNIA / NIE PEŁNIA**WYMAGANIA ZAMAWIAJACEGO |
| **Parametry systemu**Poszczególne elementy wchodzące w skład systemu muszą zapewniać obsługę: |
|  | 4 wirtualnych interfejsów sieciowych. |  |
|  | Możliwość uruchomienia w środowiskach: Microsoft Hyper-V Server 2010, 2012 R2 oraz 2016; VMware ESXi, ESX wersje:4,5,6; KVM, Xen, Microsoft Azure, AWS, Oracle OCI. |  |
| **Parametry wydajnościowe i licencyjne**System musi obsługiwać co najmniej: |
|  | Uwierzytelnianie dla 100 użytkowników. |  |
|  | 200 tokenów dla uwierzytelniania dwuskładnikowego. |  |
|  | 30 klientów protokołu RADIUS (urządzeń NAS, które można podpiąć do systemu). |  |
|  | Możliwość zdefiniowania co najmniej 10 grup użytkowników, |  |
|  | 5 lokalnych centrów certyfikacji (CA). |  |
|  | Możliwość wygenerowania 100 certyfikatów dla użytkowników. |  |
| **Wymagania ogólne**System musi zapewniać nie mniej niż: |
|  | Możliwość pracy w konfiguracji HA (High Availability) z trybem Active-Passive lub Active-Active w celu zwiększenia niezawodności. |  |
|  | Graficzną reprezentację statusu uwierzytelnionych użytkowników. |  |
|  | Logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia oraz nazwą użytkownika:a. Lokalnie.b. Zdalnie w oparciu o protokół Syslog. |  |
|  |   Konfigurację Captive Portalu. |  |
|  |
| **Wymagania funkcjonalne – uwierzytelnianie**Celem realizacji funkcji uwierzytelniających, system musi zapewniać nie mniej niż: |
|  | Lokalną, wbudowaną bazę użytkowników. |  |
|  | Przechowywanie następujących informacji o użytkowniku: nazwa, imię i nazwisko, adres email, numer telefonu, adres, kraj, województwo. |  |
|  | Możliwość zdefiniowania co najmniej 3 indywidualnie konfigurowalnych pól dla każdego z użytkowników. |  |
|  | Możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV. |  |
|  | Konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie:a.   poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych),b.    czasu ważności hasła, |  |
|  | Konfigurowalną politykę blokowania kont, która będzie uwzględniać:a.    ilość nieudanych logowań,b.    czas blokowania konta,c.     okres nieaktywności, po którym konto jest blokowane. |  |
|  | Możliwość odzyskiwania haseł:a.    z wykorzystaniem adresu email,b.    z wykorzystaniem pytania pomocniczego |  |
|  | Obsługę protokołu RADIUS zgodną z RFC, w tym zakresie system musi oferować:a.    wbudowany serwer RADIUS,b.    integrację z zewnętrznymi serwerami RADIUS – praca jako klient. |  |
|  | Obsługę protokołu LDAP, w tym zakresie system musi oferować:a.   wbudowany serwer LDAP,b.   możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP). |  |
|  | Obsługę protokołu SAML - Identity Provider (IdP) proxy. |  |
|  | Realizację funkcji SSO (Single Sign On) w oparciu o:a.  integrację z Active Directory, również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny,b.  dedykowaną aplikację instalowaną na stacjach roboczych z systemem Windows,c.   kontekst użytkownika przesyłany z serwera RADIUS,d.   informacje uzyskiwane poprzez protokół Syslog, |  |
| **Wymagania funkcjonalne – uwierzytelnianie dwuskładnikowe**Realizując uwierzytelnianie dwuskładnikowe, system musi zapewniać nie mniej niż: |
|  | Obsługę dla tokenów sprzętowych (hardware):a.   wspomniane tokeny muszą pochodzić od tego samego producenta co system uwierzytelniania. |  |
|  | Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile. |  |
|  | Dla tokenów na system iOS i Android wymaga się:a. aktywacji z centralnego systemu uwierzytelniania (seed provisioning),b.  możliwości konfiguracji ilości generowanych cyfr (6 lub 8),c.   generowania kodu (cyfr) co 30 lub 60 sekund,d.   możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne),e.  ochrony dostępu poprzez konfigurowalny kod PIN, |  |

**Możliwość integracji z logowaniem do systemu Windows.**

|  |
| --- |
| **Wymagania funkcjonalne – 802.1x**System powinien umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, spełniając nie mniej niż następujące warunki: |
|  | Obsługa co najmniej poniższych protokołów EAP:a.       PEAP,b.       EAP-TTLS,c.       EAP-TLS,d.       EAP-GTC. |  |
|  | Wsparcie dla uwierzytelnienia w oparciu o adres MAC (MAC based authentication). |  |
|  | Zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach PEAP, TTLS, TLS. |  |
| **Wymagania funkcjonalne – zarządzanie certyfikatami**System powinien spełniać następujące wymagania w zakresie zarządzania certyfikatami, nie mniej niż: |
|  | Obsługa wbudowanego CA (Certificate Authority). |  |
|  | Obsługa CA pośredniczących (Intermediate CA). |  |
|  | Ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego. |  |
|  | Możliwość pobrania wygenerowanych certyfikatów. |  |
|  | Możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP. |  |
|  | Możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP. |  |
|  | Możliwość generowania certyfikatów typu wildcard. |  |
|  | Realizacja CRL (Certificate Revocation List). |  |
|  | Wsparcie dynamicznego odwoływania certyfikatówz wykorzystaniem protokołu OCSP (RFC2560). |  |
|  | Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych. |  |
| **Zarządzanie** |
|  | Zarządzanie w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki. |  |
|  | System udostępnia graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS. |  |
|  | Tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego interfejsu zarządzającego (GUI) oraz na zewnętrzny serwer FTP/SFTP w oparciu o harmonogram, który będzie umożliwiał wskazanie konkretnego czasu kiedy proces ma się rozpocząć |  |
|  | Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych. |  |
| **Serwis, szkolenia i usługi** |
|  | Wymaga się aby dostawa obejmowała również serwis producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. | PROSZĘ WPISAĆ OFEROWANY CZAS WSPARCIA I GWARANCJA (KRYTERIUM OCENY OFERT) |
|  |
| **Dodatkowe wymogi** |
|  | Wymaga się aby dostawa obejmowała również 25 szt. tokenów dla uwierzytelniania dwuskładnikowego w formie elektronicznej licencji możliwej do zainstalowania na urządzeniach mobilnych z systemami operacyjnymi : iOS, Android i Windows Phone. |  |

# **Centralny system logowania, raportowania i korelacji.**

**Wymagania Ogólne**

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

|  |
| --- |
| **Interfejsy, Dysk:** |
|  | System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 3 TB. |  |
| **Parametry wydajnościowe:** |
|  | System musi być w stanie przyjmować minimum 5 GB logów na dzień. |  |
|  | Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów. |  |
| **W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:** |
| **Logowanie** |  |
|  | Podgląd logowanych zdarzeń w czasie rzeczywistym. |  |
|  | Możliwość przeglądania logów historycznych z funkcją filtrowania.  |  |
|  | System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:a. Listę najczęściej wykrywanych ataków.b. Listę najbardziej aktywnych użytkowników.c. Listę najczęściej wykorzystywanych aplikacji.d. Listę najczęściej odwiedzanych stron www.e. Listę krajów , do których nawiązywane są połączenia.f. Listę najczęściej wykorzystywanych polityk Firewall.g. Informacje o realizowanych połączeniach IPSec. |  |
|  | Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. |  |
|  | Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. |  |
|  | System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy. |  |
| **Raportowanie**W zakresie raportowania system musi zapewniać: |  |
|  | Generowanie raportów co najmniej w formatach: PDF, CSV. |  |
|  | Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. |  |
|  | Funkcję definiowania własnych raportów.  |  |
|  | Możliwość spolszczenia raportów. |  |
|  | Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email. |  |
| **Korelacja logów**W zakresie korelacji zdarzeń system musi zapewniać: |  |
|  | Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. |  |
|  | Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. |  |
|  | Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:* Malware.
* Aplikacje sieciowe.
* Email.
* IPS.
* Traffic.
* Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
 |  |
|  | Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.  |  |
| **Zarządzanie** |  |
|  | System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. |  |
|  | System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi. |  |
| **Serwisy i licencje** |  |
|  | System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. |  |
|  | Wsparcie: System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. | PROSZĘ WPISAĆ OFEROWANY CZAS WSPARCIA I GWARANCJA (KRYTERIUM OCENY OFERT) |
|  |

# **Oprogramowanie Antywirusowe**

|  |
| --- |
| **Zaawansowana ochrona stacji roboczych – rozbudowa obecnego systemu.**Przedmiotem postępowania jest rozbudowa istniejącego systemu bezpieczeństwa infrastruktury teleinformatycznej o elementy zabezpieczeń dla stacji roboczych wraz z mechanizmami centralnego zarządzania. |
|  | Dostarczone rozwiązanie do ochrony stacji roboczych musi zapewniać wszystkie wymienione poniżej funkcje i mechanizmy. Dopuszcza się aby poszczególne elementy wchodzące w skład rozwiązania były zrealizowane w postaci osobnych, komercyjnych platform lub komercyjnych aplikacji. |  |
| **System ochrony dla stacji roboczych wraz z systemem centralnego zarządzania.** |
|  | W ramach postepowania wymaganym jest dostarczenie rozwiązania do ochrony stacji roboczych wraz z mechanizmami centralnego zarządzania.Dostarczone rozwiązanie do ochrony stacji roboczych musi zapewniać wszystkie wymienione poniżej funkcje i mechanizmy. Dopuszcza się aby poszczególne elementy wchodzące w skład rozwiązania były zrealizowane w postaci osobnych, komercyjnych platform lub komercyjnych aplikacji. |  |
| **Parametry systemu ochrony dla stacji roboczych:** |
| Elementy systemu ochrony dla stacji roboczych powinny zapewniać następujące funkcje i mechanizmy: |  |
|  | Kontrola antywirusowa. |  |
|  | Funkcja analizy plików w zewnętrznym systemie Sandbox. |  |
|  | Opcja kwarantanny lokalnej plików przesłanych do Sandbox na czas analizy. |  |
|  | URL filtering w oparciu o kategorie stron z opcją definiowania wyjątków.  |  |
|  | Kontrola aplikacji - w oparciu o wbudowany Firewall aplikacyjny. |  |
|  | Mechanizmy analizy podatności na stacji roboczej - pozwalające wykryć zagrożenia w systemie operacyjnym oraz zainstalowanych aplikacjach. |  |
|  |  |
|  | Mechanizmy szyfrowanych połączeń typu IPSec VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu. |  |
|  | Mechanizmy szyfrowanych połączeń typu SSL VPN z opcją Split tunneling (przekierowanie tylko określonego ruchu do tunelu) oraz możliwością przekierowania całego ruchu do tunelu. |  |
|  | Możliwość zastosowania certyfikatów cyfrowych w procesie uwierzytelnienia przy realizacji szyfrowanych połączeń. |  |
|  | Mechanizmy uwierzytelniania dwuskładnikowego |  |
|  | AntiExploit,  |  |
|  | blokowanie dysków przenośnych typu USB,  |  |
|  |  |
| Poszczególne mechanizmy muszą być dostępne dla następujących systemów operacyjnych: Microsoft Windows 10 (32-bit, 64-bit), Windows 11 (32-bit, 64-bit), Windows Serwer 2019, Windows Server 2016, Windows Server 2022, Mac OS X v10.15, OS X v10.14, OS X v10.13, Linux OS, Ubuntu 16.04 i późniejsze, Red Hat 7.4 i późniejsze, CentOS 7.4 i późniejsze. |  |
| Wymaganym jest aby system ochrony stacji końcowej umożliwiał wysyłanie plików do platformy typu Sandbox zlokalizowanego w chmurze producenta (co najmniej w ilości 300 plików dziennie dla każdej stacji klienckiej) lub w ramach postępowania powinna zostać dostarczona komercyjna platforma typu sandbox - zainstalowana lokalnie i współpracująca z oferowanym rozwiązaniem do ochrony stacji roboczych. W ramach postępowania muszą zostać dostarczone niezbędne licencje upoważniająca zrealizowania wymaganej powyżej funkcji. |  |
| **Parametry systemu centralnego zarządzania.** |
|  | Dostarczony system centralnego zarządzania aplikacjami klienckimi musi zapewniać wszystkie wymienione poniżej funkcje. Wymaga się aby elementy wchodzące w skład systemu były zrealizowane w postaci komercyjnych platform wirtualnych lub aplikacji instalowanych na systemach operacyjnych: Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows Server 2022. |  |
|  | System powinien umożliwiać automatyczną aktualizację oprogramowania zabezpieczającego na urządzeniach końcowych oraz musi zapewniać mechanizmy integracji z sieciowymi systemami bezpieczeństwa, w tym co najmniej: Firewall, Sandbox. |  |
| Ponadto wymagane jest aby system zapewniał: |  |
|  | integrację z systemami zarządzania tożsamością użytkowników – co najmniej AD, |  |
|  | definiowanie różnych profilów (wersji konfiguracji) ochrony dla różnych grup użytkowników czerpanych z AD lub definiowanych lokalnie, |  |
|  | zautomatyzowany proces zarządzania aplikacja kliencką, |  |
|  |  |
|  | przygotowywanie paczek instalacyjnych przynajmniej dla systemu Windows 32/64 bit i MacOS w których administrator może określić komponenty dla ochrony stacji roboczych takich jak AV, WebFiler, Skaner Podatności. |  |
|  | możliwość edycji pliku konfiguracyjnego w zewnętrznym edytorze tekstowym, |  |
|  | panel, w którym wyświetlane są wyniki analizy podatności na stacjach roboczych, |  |
|  | panel w którym wyświetlane są informacje o podłączonych i zarządzanych stacjach roboczych, |  |
|  | możliwość wymuszenia patchowania wykrytych podatności na stacjach roboczych, |  |
|  | automatyczne wykrywanie stacji klienckich w grupach roboczych, |  |
|  | logowanie zdarzeń z aplikacji klienckich, możliwość ich przeglądania z funkcja filtrów oraz możliwością pobierania logów przez administratora, |  |
|  | generowanie alarmów: związanych z zarządzeniem aplikacją kliencką, w przypadku wykrycia ważnych podatności na stacjach oraz w sytuacji zaistnienia zdarzeń związanych z aktywnością złośliwego kodu, aktywności aplikacji botnet z wykorzystaniem komunikacji C&C, nieaktualnej bazy danych dla sygnatur antywirusa.  |  |
|  | definiowanie grup administratorów lokalnie oraz w oparciu o AD z opcja przypisywania uprawnień do elementów panelu konfiguracyjnego, |  |
|  | zarządzenie certyfikatami na potrzeby połączeń IPSec VPN oraz SSL VPN, |  |
|  | automatyczne wykrywanie aplikacji zainstalowanych na stacjach klienckich z możliwością filtrowania przynajmniej po producencie i nazwie aplikacji, |  |
|  | możliwość przeniesienia użytkownika przez administratora do kwarantanny i personalizację komunikatu, który wyświetli się użytkownikowi, |  |
|  | możliwość wymuszenia przeskanowania stacji klienckiej za pomocą antywirusa i skanera podatności na żądanie jak i cyklicznie, |  |
|  | możliwość skonfigurowania weryfikacji zgodności (compliance) w celu sprawdzenia czy na stacji końcowej jest aktualna baza sygnatur dla AV, czy jest odpowiednia wersja systemu operacyjnego, czy jest uruchomiony odpowiedni proces. |  |
| Administrator musi mieć możliwość wykonywania backupu i odtwarzania bazy danych, w oparciu o którą działają elementy system. |  |
| Centralny system zarządzania musi zapewniać możliwość dystrybucji paczek instalacyjnych z lokalnych zasobów w oparciu o adres URL definiowany przez administratora lub w ramach postępowania koniecznym jest dostarczenie odpowiednio zabezpieczonego portalu, za pośrednictwem którego administrator będzie mógł dystrybuować paczki instalacyjne. |  |
| **Licencje oraz serwisy** W ramach postępowania wraz z konsolą centralnego zarządzania muszą zostać dostarczone niezbędne licencje upoważniające do: |
|  | Zainstalowania i centralnego zarządzania aplikacjami klienckimi na 75 stacjach roboczych.  |  |
|  | Dla wskazanej powyżej ilości stacji roboczych licencje powinny obejmować:1. Kontrola Aplikacji, Antywirus, Web Filtering, Skaner podatności, Software inventory, Remote Access, Threat Outbreak Detection, Sandbox Agent with Cloud Sandbox subscription,

centralne zarządzanie **na okres 36 miesięcy.**  |  |
| System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. | PROSZĘ WPISAĆ OFEROWANY CZAS WSPARCIA I GWARANCJA (KRYTERIUM OCENY OFERT) |
|  |

# **System ochrony poczty elektronicznej**

|  |
| --- |
| **Wymagania ogólne** |
|  | System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników. |  |
|  | Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systememu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure. |  |
|  | Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.  |  |
| Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów: |  |
|  | Tryb Gateway. |  |
|  | Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej). |  |
| **Parametry fizyczne systemu antyspamowego** |
|  | System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 2 TB. |  |
| **Ogólne funkcje systemu ochrony poczty**Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje: |
|  | Wsparcie dla co najmniej 100 domen pocztowych. |  |
|  | System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 50 tys. wiadomości/godzinę. |  |
|  | Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all). |  |
|  | Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP. |  |
|  | Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości). |  |
|  | 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. |  |
|  | Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej. |  |
|  | Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów. |  |
|  | Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP. |  |
|  | Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika. |  |
|  | Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora. |  |
|  | Dostęp do kwarantanny użytkownika możliwy poprzez WebMail. |  |
|  | Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki. |  |
|  | Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI. |  |
|  | Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu. |  |
|  | Białe i czarne listy adresów mailowych dla poszczególnych użytkowników. |  |
|  | Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Preention). |  |
|  | Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika. |  |
| **Kontrola antywirusowa i ochrona przed malware**W tym zakresie dostarczony system ochrony poczty musi zapewniać: |
|  | Skanowanie antywirusowe wiadomości SMTP. |  |
|  | Kwarantannę dla zainfekowanych plików. |  |
|  | Skanowanie załączników skompresowanych.  |  |
|  | Definiowanie komunikatów powiadomień w języku polskim. |  |
|  | Blokowanie załączników w oparciu o typ pliku. |  |
|  | Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antywirusowej. |  |
|  | Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu. |  |
|  | Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. |  |
|  | Ochronę typu wirus outbrake.  |  |
|  | Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.  |  |
| **Kontrola antyspamowa** System musi zapewniać poniższe funkcje i metody filtrowania spamu: |
|  | Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta. |  |
|  | Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania. |  |
|  | Szczegółowa kontrola nagłówka wiadomości.  |  |
|  | Analiza Heurystyczna. |  |
|  | Współpraca z zewnętrznymi serwerami RBL, SURBL. |  |
|  | Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen. |  |
|  | Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników. |  |
|  | Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.  |  |
|  | Kontrola w oparciu o Greylisting oraz SPF. |  |
|  | Filtrowanie treści wiadomości i załączników. |  |
|  | Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości. |  |
|  | Możliwość zdefiniowania nie mniej niż 200 polityk kontroli antyspamowej. |  |
|  | Ochrona typu outbrake. |  |
|  | Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).  |  |
|  | Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.  |  |
|  | Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level)  |  |
|  | Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. |  |
| **Ochrona przed atakami na usługę poczty**System musi zapewniać poniższe funkcje i metody filtrowania: |
|  | Ochrona przed atakami na adres odbiorcy (m.in. email bombing). |  |
|  | Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.  |  |
|  | Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu. |  |
|  | Kontrola Reverse DNS (ochrona przed Anty-Spoofing). |  |
|  | Weryfikacja poprawności adresu e-mail nadawcy. |  |
| **Funkcje logowania i raportowania**W tym zakresie dostarczony system ochrony poczty musi zapewniać: |
|  | Logowanie do zewnętrznego serwera SYSLOG. |  |
|  | Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku. |  |
|  | Logowanie informacji na temat spamu oraz niedozwolonych załączników. |  |
|  | Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych. |  |
|  | Możliwość analizy przebiegu sesji SMTP. |  |
|  | Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych. |  |
|  | Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.  |  |
|  | Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.  |  |
| **Funkcje pracy w trybie wysokiej dostępności (HA)**System ochrony poczty musi zapewniać poniższe funkcje: |
|  | Konfigurację HA w każdym z trybów: gateway, transparent. |  |
|  | Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP. |  |
|  | Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu. |  |
|  | Monitorowanie stanu pracy klastra. |  |
| **Aktualizacje sygnatur, dostęp do bazy spamu** W tym zakresie dostarczony system ochrony poczty musi zapewniać: |
|  | Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym. |  |
|  | Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę. |  |
| **Zarządzanie** System ochrony poczty musi zapewniać poniższe funkcje: |
|  | System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH. |  |
|  | Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy. |  |
|  | Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych. |  |
| **Certyfikaty**Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji: |
|  | VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified. |  |
| **Serwisy i licencje** System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: |
|  | Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise **na okres 36 miesięcy.**  |  |
| **Wsparcie** |
| System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.  | PROSZĘ WPISAĆ OFEROWANY CZAS WSPARCIA I GWARANCJA (KRYTERIUM OCENY OFERT) |
|  |

W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien 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.

Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż posiada on autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

**CZĘŚĆ 1 -AUDYT**

# **Audyt bezpieczeństwa**

Wykonawca po wdrożeniu systemów teleinformatycznych wykona audyt końcowy sprawdzający podniesienie poziomu bezpieczeństwa systemów teleinformatycznych zamawiającego w oparciu
o wymagania Ustawy o Krajowym Systemie Cyberbezpieczeństwa,

Celem audytu jest wykazanie przez świadczeniodawcę podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności, **zgodnie z zarządzeniem nr 68/2022/BBIICD
Prezesa Narodowego Funduszu Zdrowia z dnia 20 maja 2022 r.** **(**[**https://baw.nfz.gov.pl/NFZ/document/319/Zarz%C4%85dzenie-68\_2022\_BBIiCD**](https://baw.nfz.gov.pl/NFZ/document/319/Zarz%C4%85dzenie-68_2022_BBIiCD) **)** Oraz w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa u świadczeniodawcy
w formie ankiety.

Przeprowadzony audyt ma wykazać podniesienie poziomu bezpieczeństwa teleinformatycznego
w odniesieniu do poziomu wynikającego z ankiety lub jego brak.

Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły pozytywnie na podniesienie poziomu bezpieczeństwa.

Oświadczam, że wszystkie wymagania całości zamówienia (część nr 1, część nr 2) zostały przeze mnie spełnione

………………………………………

*(data i podpis osoby upoważnionej)*