*Załącznik nr 1 do SWZ – Szczegółowy opis przedmiotu zamówienia*

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

**DOSTAWA I WDROŻENIE MECHANIZMÓW AUTENTYKACJI PRACY I SYSTEMU OCHRONY POCZTY**

1. **Zakup i wdrożenie systemu ochrony poczty**

# **Wymagania ogólne**

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o dedykowany system operacyjny oraz komercyjne bazy zabezpieczeń.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:

1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

# **Parametry systemu antyspamowego**

1. System musi mieć możliwość alokacji wirtualnych interfejsów:
* do 4 vNIC.
1. System musi mieć możliwość alokacji storage 250 GB do 1 TB.
2. System musi mieć możliwość alokacji do 1 vCPU

# **Ogólne funkcje systemu ochrony poczty**

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:

1. Wsparcie dla co najmniej 20 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 30 tys. wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. 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.
7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
11. Możliwość poddania ponownemu skanowaniu (antywirus, antyspam, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail oraz POP3.
13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
17. Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Preention).
18. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.
19. Możliwość integracji z Office 365 oraz serwerami Exchange z wykorzystaniem API.

# **Kontrola antywirusowa i ochrona przed malware**

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 200 profili kontroli antywirusowej.
7. 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.
8. 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.
9. Ochronę typu wirus outbreak.
10. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MSOffice, 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:

1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 200 profili kontroli antyspamowej.
13. Ochrona typu outbreak.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.
16. Możliwość wykrywania i ochrony przed podszywaniem sie (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level)
17. 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:

1. Ochrona przed atakami na adres odbiorcy.
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

# **Funkcje logowania i raportowania**

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. 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:

1. Konfigurację HA w każdym z trybów: gateway, transparent.
2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.
3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
4. Monitorowanie stanu pracy klastra.

# **Aktualizacje sygnatur, dostęp do bazy spamu**

W tym zakresie dostarczony system ochrony poczty musi zapewniać:

1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

# **Zarządzanie**

System ochrony poczty musi zapewniać poniższe funkcje:

1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 10 lokalnych kont administracyjnych.

# **Certyfikaty**

1. VBSpam and VB100 rated lub Common Criteria NDPP, FIPS 140-2 Certified.

**Serwisy i licencje**

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 **24 miesięcy**

# Gwarancja oraz wsparcie

Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Od Wykonawcy wymaga się wdrożenia dostarczonego rozwiązania wraz z pełną konfiguracją polityk bezpieczeństwa i integracją z infrastrukturą informatyczną Zamawiającego.
Wdrożenie musi być przeprowadzone przez certyfikowanego inżyniera, posiadającego minimum 4 aktywne certyfikaty producenta oferowanego w postępowaniu rozwiązania UTM w zakresie:
• Certyfikat w zakresie Bezpieczeństwa Sieci (NS)
• Certyfikat w zakresie Bezpieczeństwa Chmury Publicznej (PCS)
• Certyfikat w zakresie Operacji Bezpieczeństwa (SO)
• Certyfikat w zakresie Dostępu na Krawędzi Sieci (SASE)

1. **Zakup i wdrożenie mechanizmów autentykacji pracy**

|  |  |  |
| --- | --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  | **Parametry sprzętu****oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**) |
| **Typ** | **Mobilne urządzenie do uwierzytelniania dwuskładnikowego, fabrycznie nowe** |
| Rozwiązanie | Mobilne urządzenie do uwierzytelniania dwuskładnikowego | ………………. |
| Licencja | wieczysta licencja na tokeny, brak opłat za subskrypcje  | ………………. |
| Dzaiałania | Wspierane platformy: FortiClient, FortiAuthenticator, generowanie haseł bez potrzeby instalowania oprogramowania klienckiego,  | ………………. |
| **Zgodne algorytmy** | Zgodność z OATH,TOTP | …………………. |
| **Wyświetlacz** | LCD wysokiego kontrastu, min. 6 cyfr | …………………. |
| **Zasilanie** | Bateria, min. żywotność baterii - min. 3 lata | …………………. |
| **Dostępne informacje na wyświetlaczu LCD** | Timer pokazujący czas pozostały do następnej generacji OTP | …………………. |
| **Generator haseł** | zgodny z FIPS 140-2 | …………………. |
| **Czas zmiany hasła i wygenerowania kolejnego** | Min. 2 opcje, możliwe opcje min.: co 30 s. oraz co 60s. |  |
| **Wymiary** | Max. 65x30x10 mm | …………………. |
| **Stopień ochrony** | Min IP65 | …………………. |
| Standarty | Min.: OATH-TOTP (RFC6238) HMAC-SHA1 | …………………. |
| **Certyfikaty i zgodność** | RoHS, CE, FCC, ICES, UKCA | …………………. |
| **Temperatura pracy zakres** | 10°-40°C | …………………. |

1. **Zakup i wdrożenie mechanizmów autentykacji pracy mobilnej**

|  |  |  |
| --- | --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne**  | **Parametry sprzętu****oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**) |
| **Typ** | **Licencja na tokeny do uwierzytelnienia dwuskładnikowego w postaci licencji elektronicznej dla aplikacji na urządzenia mobilne.** |
| Rozwiązanie | Licencja na tokeny do uwierzytelniania dwuskładnikowego | ………………. |
| Licencja | wieczysta licencja na tokeny, brak opłat za subskrypcje  | ………………. |
| Dzaiałania | Wspierane platformy: FortiClient, FortiAuthenticator, generowanie haseł | ………………. |
| **Generator haseł** | Zgodny OTP i czasowym OATH | ………………. |
| **Wspierane plattformy** | iOS , Android , Windows Phone 8/8.1, Windows 10 I Windows Uniwersalna Platforma , | ………………. |
| **Specyfikacja OTP**  | FC 6238, RFC 4226 | ………………. |
| **Zatwierdzenie jednym dotknięciem**  | Dane logowania przesłane na urządzenie przenośne, zatwierdzane jednym kliknięciem  | ………………. |
| **Certyfikat bezpieczeństwa aplikacji mobilnych** | Min. v3.1 dla urządzeń z Androidem i iOS | ………………. |
| **Przenoszenie kodu** | Możliwość skopiowania kodu OTP do schowka urządzenia | ………………. |
| Zabezpieczenie aplikacji | kodem PIN lub odciskiem palca | ………………. |
| **Weryfikacja Serial Number**  | Możliwa do sprawdzenia na urządzeniu | ………………. |