Wydatek współfinansowany z Europejskiego Funduszu Społecznego



**Załącznik nr 1**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**I. Opis przedmiotu zamówienia:**

1. Świadczenie usług wsparcia technicznego dla posiadanego przez Zamawiającego systemu antyspamowego, przez 12 miesięcy. Zamawiający posiada aktualnie system „FortiMail-VM01 24x7 FortiCare and FortiGuard Base Bundle Contract”. Aktualne wsparcie techniczne wygasa w dniu 09.12.2019 r. Zamawiający dopuszcza możliwość przedłużenia wsparcia dla posiadanego rozwiązania, jak również zaoferowanie rozwiązania równoważnego, pod warunkiem, iż będzie możliwe do zastosowania dla posiadanego systemu. Warunki równoważności opisano w pkt III Szczegółowego Opisu Przedmiotu Zamówienia. W ramach pakietu wsparcia Zamawiający w okresie od 10.12.2019 do 09.12.2020 ma prawo do:
2. Wsparcia służb technicznych producenta  - 24x7 – diagnostyka błędów w oprogramowaniu
3. Subskrypcji sygnatur zagrożeń dla AntiSpam i Antivirus
4. W terminie 7 dni od dnia zawarcia Umowy Wykonawca zarejestruje pakiet wsparcia technicznego, na stronie internetowej Producenta Oprogramowania. O fakcie zarejestrowania, Wykonawca powiadomi Zamawiającego drogą elektroniczną.
5. W ramach Umowy Wykonawca będzie świadczył Zamawiającemu usługi eksperckie w ilości 60 roboczogodzin w zakresie świadczenia obsługi technicznej Oprogramowania i wsparcia administratorów Zamawiającego, zwanych dalej „Usługami” obejmujących:
6. przyjmowanie zgłoszeń w zakresie awarii i problemów z Oprogramowaniem;
7. usuwanie awarii i rozwiązywanie problemów z Oprogramowaniem, zgłoszonych przez Zamawiającego;
8. udzielanie administratorom Zamawiającego wsparcia w postaci porad i wyjaśnień dotyczących Oprogramowania;
9. instruowanie administratorów Zamawiającego w zakresie działania oprogramowania;

**II. Usługi eksperckie :**

1. Usługi świadczone będą co do zasady telefonicznie oraz poprzez zdalny dostęp do systemów informatycznych za pomocą VPN. Zasady korzystania z VPN zostały opisane w załączniku nr 3 do Umowy.
2. W przypadku, gdy będzie to konieczne, Usługi świadczone będą również w siedzibie Zamawiającego.
3. Strony ustalają następujące priorytety zgłoszeń:
4. **priorytet niski** - dotyczy zgłoszeń nie zakłócających pracy Zamawiającego, w szczególności zmian w konfiguracji, wdrożenia nowych funkcjonalności;
5. **priorytet ważne** - dotyczy zgłoszeń istotnie utrudniających pracę Zamawiającego, niedostępności części funkcjonalności Oprogramowania;
6. **priorytet krytyczne** - dotyczy zgłoszeń uniemożliwiających pracę Zamawiającego, niedostępności całkowitej Oprogramowania;
7. Zgłoszenia dokonywane będą za pośrednictwem poczty elektronicznej na adres ………………………. Zgłoszenia o priorytecie krytyczne zgłaszane będą dodatkowo telefonicznie na numer
……….. Zgłoszenia mogą być dokonywane w dni robocze[[1]](#footnote-1) w godzinach 8-17. Zgłoszenia dokonane poza tymi godzinami przyjmuje się za dokonane w następnym dniu, w którym zgodnie ze zdaniem poprzedzającym Wykonawca zobowiązany jest do ich przyjmowania.
8. Strony ustalają następujące czasy reakcji dla poszczególnych priorytetów zgłoszeń:
9. priorytet niski – max 6 godziny od zgłoszenia;
10. priorytet ważne – max 6godziny od zgłoszenia;
11. priorytet krytyczne – max 4 godziny od zgłoszenia (czas wskazany w Ofercie Wykonawcy i oceniany w ramach kryterium).
12. Zgłoszenie powinno obejmować następujące dane:
13. osobę zgłaszającą;
14. priorytet zgłoszenia;
15. opis sytuacji;
16. opis dotychczas podjętych działań i ich dotychczasowe rezultaty.
17. Przez czas reakcji Strony przyjmują maksymalny czas, jaki powinien upłynąć od momentu dokonania zgłoszenia, o którym mowa w ust. 4 do rozpoczęcia działań ze strony Wykonawcy.
18. Strony ustalają następujące czasy zakończenia zgłoszenia liczącego od momentu zakończenia przewidywanego czasu reakcji dla poszczególnych priorytetów zgłoszeń:
19. priorytet niski – max 24 godziny;
20. priorytet ważne – max 12 godziny;
21. priorytet krytyczne – max 8 godzin (czas wskazany w Ofercie Wykonawcy i oceniany w ramach kryterium)
22. Działania Wykonawcy podejmowane będą w dni robocze w godzinach 8-17.
23. Zamawiający zastrzega sobie możliwość żądania wstrzymana działań przez Wykonawcę, żądania kierowane będą na adres poczty elektronicznej lub numer telefonu określone w ust. 4.
24. W przypadku, o którym mowa w ust. 10 Zamawiający będzie zobowiązany do zapłaty wynagrodzenia za usługi świadczone do momentu zgłoszenia żądania wstrzymania działań
25. Na dzień podpisania umowy Wykonawca deklaruje, że w skład zespołu specjalistów Wykonawcy świadczących Usługi na rzecz Zamawiającego wchodzić będą ………………………………………………………………………………………..……….. Wykonawca ma prawo do zmiany osób świadczących Usługi na rzecz Zamawiającego na inne osoby o odpowiedniej wiedzy i doświadczeniu po uprzednim uzyskaniu zgody Zamawiającego. Zamawiający ma prawo do żądania zmiany osób świadczących Usługi.
26. W przypadku konsultacji telefonicznych lub przy pomocy komunikatora Skype czas rozmowy liczony będzie w ten sposób, że rozmowa do 30 minut liczona będzie jako 50% stawki za roboczogodzinę, a powyżej 30 minut do 60 minut jako pełna stawka za roboczogodzinę.
27. Po zakończonym miesiącu kalendarzowym świadczenia usług w ramach niniejszej Umowy Wykonawca prześle Zamawiającemu raport, który będzie wyszczególniać co najmniej:
28. rodzaj wykonanych w danym miesiącu kalendarzowym zadań (naprawa błędów, konsultacje telefoniczne lub przy pomocy komunikatora Skype, konsultacje przez e-mail lub pisemnie, aktualizacja oprogramowania itp.),
29. datę/okres wykonania danego zadania,
30. czas poświęcony na wykonanie poszczególnych zadań
31. Raport powinien być przekazany co najmniej w formie elektronicznej na każdy z adresów e-mail podanych do komunikacji w § 8 Umowy.
32. Celem usunięcia wątpliwości Strony zgodnie oświadczają, że czas dojazdu do siedziby Zamawiającego nie wlicza się do czasu pracy.

**III. Warunki równoważności:**

Zamawiający dopuszcza, aby w ramach realizacji przedmiotu zamówienia, Wykonawca, który nie może zapewnić wymaganych usług dla posiadanego przez Zamawiającego rozwiązania, w cenie wskazanej w ofercie, dostarczy inny system, oparty o odpowiednie rozwiązania techniczne, w ramach którego zobowiązany będzie do realizacji usług opisanych w SOPZ. Aktualny system posiadany przez Zamawiającego charakteryzuje się poniższymi parametrami. W przypadku skorzystania z tej opcji, system zapewniony przez Wykonawcę musi posiadać parametry nie gorsze niż system Zamawiającego:

|  |  |  |
| --- | --- | --- |
|  | **Parametry podstawowe** | **Opis**  |
|  | Architektura systemu ochrony | System ochrony musi zapewniać kompleksową ochronę antyspamową, antywirusową i antyspyware’ową. (licencja na urządzenie). System musi być dostarczony w postaci komercyjnej platformy działającej w środowisku wirtualnym z możliwością uruchomienia na posiadanych przez Zamawiającego hypervisorach Microsoft Hyper-V 2012 R2  |
|  | Sposoby implementacji | System powinien mieć możliwość pracy w każdym z trzech trybów:* Tryb gateway
* Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej)

Tryb serwera pocztowego |
|  | Funkcjonalności | System musi realizować poniższe funkcjonalności w każdym z trzech trybów pracy:* Wsparcie dla wielu domen pocztowych
* Polityki filtrowania tworzone w oparciu o adresy mailowe, nazwy domenowe, adresy IP (w szczególności reguła all-all)
* Email routing oraz zarządzanie kolejkami bazujące na politykach
* Ochrona poczty przychodzącej oraz wychodzącej
* Granularne, wielowarstwowe polityki wykrywania spamu oraz wirusów
* Skanowanie Antywirusowe oraz Antyspamowe definiowane na użytkownika w oparciu o atrybuty LDAP
* Routing poczty (email routing) w oparciu o LDAP
* Kwarantanna poczty z dziennym podsumowaniem (możliwość samodzielnego zwalniania plików z kwarantanny przez użytkownika)
* Dostęp do kwarantanny poprzez WebMail lub POP3
* Uwierzytelnianie SMTP w oparciu o protokoły: LDAP, RADIUS, POP3, IMAP
* Mechanizmy reputacji nadawcy wiadomosci

Whitelist’y definiowane dla użytkownika |
|  | Funkcjonalności w trybie serwera pocztowego | System musi zapewniać:* Obsługę serwisów pocztowych: SMTP, POP3, IMAP
* Wsparcie SMTP over SSL
* Definiowanie powierzchni dyskowej dla użytkowników
* Szyfrowany dostęp do poczty poprzez WebMail
* Polski interfejs użytkownika przy dostępie przez WebMail
* Kalendarz na WebMail’u
* Lokalne konta użytkowników oraz uwierzytelnianie w oparciu o LDAP
* Synchronizacja książki adresowej z LDAP
 |
|  | Ochrona antywirusowa, antyspyware’owa | System musi realizować:* Skanowanie antywirusowe wiadomości SMTP
* Kwarantannę dla zainfekowanych plików
* Skanowanie załączników skompresowanych
* Definiowanie komunikatów powiadomień w języku polskim
* Blokowanie załączników ze względu na typ pliku
 |
|  | Ochrona antyspamowa | System musi zapewniać poniższe metody filtrowania spamu:* + Heurystyczna analiza poczty z dynamiczną aktualizacją reguł
	+ Filtrowanie treści załączników, filtrowanie wiadomości po słowach kluczowych
	+ Szczegółowa kontrola nagłówka wiadomości
	+ Filtrowanie w oparciu o filtry Bayes’a, z możliwością dostrajania dla poszczególnych użytkowników
	+ Filtrowanie poczty w oparciu o sumy kontrolne spamu
	+ Wykrywanie spamu w oparciu a analizę plików graficznych oraz plików PDF
	+ Analiza poczty w oparciu o dynamiczną bazę spamu dostarczaną przez tego samego producenta
	+ Współpraca z zewnętrznymi serwerami RBL
	+ Kontrola w oparciu o Greylist’y
	+ Białe i czarne listy definiowane globalnie oraz per użytkownik
	+ Weryfikacja źródłowego adresu IP
	+ Mechanizmy reputacji użytkownika
* Możliwe akcje dla poczty: Accept, Relay, Reject,, Discard, Kwarnatanna, Oznaczanie (Tagging)
 |
|  | Ochrona przed atakami DoS | * Denial of Service (Mail Bombing)
* Ochrona przed atakami na adres odbiorcy
* Definiowanie maksymalnych ilości wiadomości pocztowych
* Kontrola Reverse DNS (Anty-Spoofing)
* Weryfikacja poprawności adresu e-mail nadawcy
 |
|  | Parametry wydajnościowe i niezawodnościowe | * ochrona minimum 3 domen pocztowych
* obsługa min 150 lokalnych skrzynek pocztowych w trybie serwer
* Obsługę nie mniej niż 50 profili antywirusowych lub antyspamowych
* Skanowanie Antyspamowe min. 25 000 wiadomości/godzinę (w oparciu o 100KB wiadomość)
 |
|  | Bezpieczeństwo wiadomości | * System musi zapewniać mechanizmy szyfrowania wysyłanych wiadomości pocztowych, bez konieczności instalowania jakichkolwiek aplikacji na stacjach klienckich. Administrator musi mieć możliwość włączenia tej funkcjonalności dla wybranych użytkowników.
* Wsparcie dla szyfrowanej komunikacji Gateway-to-Gateway
* Wsparcie dla szyfrowanych protokołów: HTTPS, SMTPS, IMAPS, POP3S
 |
|  | Logowanie i raportowanie | * Możliwość definiowania polityki w oparciu w wbudowany kreator konfiguracji
* Logowanie SNMP dla zdarzeń systemowych oz możliwością definiowania progów
* Logowanie do zewnętrznego serwera SYSLOG
* Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych
* Powiadamianie o działalności wirusów
* Logowanie informacji na temat spamu oraz niedozwolonych załączników
* Predefiniowane szablony raportów
* Możliwość planowania czasu generowania raportów
* Możliwość podglądu logów w czasie rzeczywistym
 |
| 1. 13.
 | Tryb wysokiej dostępności (HA) | System musi zapewniać:* Konfigurację HA [Active-Passive] w każdym z trybów: gateway, transparent, serwer
* Tryb Active-Passive z syncronizacją polityk i wiadomości, gdzie cluster występuje pod jednym adresem IP
* Tryb synchronizacji konfiguracji dla scenariuszy rozległych (osobne adresy IP)
* Wykrywanie awarii i powiadamianie administratora
* Monitorowanie stanu połączeń
 |
| 1. 14.
 | Aktualizacje sygantur, dostęp do bazy spamu | System musi zapewniać:* Pracę w oparciu o bazę spamu uaktualnianą w czasie rzeczywistym
* Planowanie aktualizacji szczepionek antywirusowych w czasie (Scheduler)

Wymuszona aktualizacja bazy wirusów (tryb push) |
| 15. | Zarządzanie i Raportowanie | * Lokalny interfejs zarządzania poprzez szyfrowane połączenie HTTPS, SSH
* Definiowanie wyglądu interfejsu zarządzania z możliwością wstawienia logo firmy
 |
| 16. | Gwarancja producenta i wsparcie serwisowe firmy wdrożeniowej | Instalacja i konfiguracja systemu musi być przeprowadzona przez uprawnionego inżyniera posiadającego odpowiedni, aktualny na dzień złożenia oferty certyfikat wystawiany przez producenta zaoferowanego oprogramowania lub certyfikat równoważny.* Wsparcie producenta w trybie 24x7 na okres minimum 12 miesięcy.
* 12 miesięczne wsparcie techniczne ze strony firmy wdrożeniowej, możliwość zgłaszania awarii w dni robocze w godzinach 8.00 - 17.00
* 12 miesięczna subskrypcja w pełnej funkcjonalności bezpieczeństwa.
 |
|  |  |  |
| 17. | Informacje dodatkowe | * System ochrony poczty bez ograniczeń licencyjnych pod względem ilości chronionych skrzynek pocztowych.
* System ochrony poczty z możliwością archiwizowania poczty.
* Możliwość współpracy systemu ochrony poczty z urządzeniami typu Sandbox w celu blokowania nieznanych zagrożeń.
* Możliwość uruchomienia systemy ochrony przed wyciekiem poufnych informacji (DLP) działający w oparciu o co najmniej reguł statyczne (słowa, wyraźnie regularne) oraz bazę dokumentów.
 |
|  |  |  |

Wykonawca musi wdrożyć oferowane rozwiązanie w zakresie:

1. Analiza obecnego systemu pod kątem wdrożenia.
2. Przygotowanie projektu technicznego wdrożenia w konfiguracji wysokiej dostępności bez pojedynczego punktu awarii.
3. Przygotowanie konfiguracji urządzenia i polityk wstępnych do uruchomienia

systemu w sieci klienta.

1. Przygotowanie schematu rekonfiguracji elementów sieci klienta.
2. Integrację wdrażanego systemu z istniejącym w infrastrukturze sieciowej klienta systemem logowania i raportowania.
3. Integracja wdrażanego systemu z posiadanym przez Zamawiającego systemu Active Directory i systemem pocztowym w celu uruchomienia weryfikacji poprawności odbiorców poczty.
4. Integrację z systemem monitoringu SNMP obsługiwanego przez Zamawiającego.
5. Uruchomienie routingu mailowego do systemu pocztowego.
6. Przygotowanie procedur reagowania na najczęściej występujące zdarzenia.
7. Wykonanie dokumentacji powdrożeniowej.
8. 8 godzinne szkolenie dla 2 użytkowników w zakresie obsługi systemu. Kwota za szkolenie wliczona jest w wynagrodzenie przysługujące z tytułu należytego wykonania Umowy w § 5 ust. 1.
1. dni robocze – dni od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy. [↑](#footnote-ref-1)