Załącznik nr 1

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

I. Specyfikacja techniczna przedmiotu zamówienia. CPV – 72532000 -3

Przedmiotem zamówienia jest dostawa i instalacja platformy sprzętowej, oprogramowania oraz usług towarzyszących, które w sumie złożą się na system ochrony antywirusowej chroniący sieć PSTD, będący uzupełnieniem użytkowanego w Policji systemu antywirusowego chroniącego stanowiska dostępowe podłączone do sieci PSTD. **W Policji do ochrony stanowisk dostępowych zastosowano system antywirusowy oparty** na **rozwiązaniu firmy Trend Micro.**

Ze względów technicznych, funkcjonalnych oraz z zasad wynikających z polityki bezpieczeństwa konieczne jest aby zakupione rozwiązanie pod względem technicznym i funkcjonalnym było inne niż **obecnie użytkowane w Policji.**

Dostarczony system musi być skalowalny tzn. musi posiadać możliwość rozbudowy.

1. Zabezpieczenie punktów styku w KGP

1.1. Sprzętowe skanery antywirusowe typu Appliance – 6 szt pracujące w układzie HA (High Availability)- w konfiguracji minimalnej:

- Obudowa – 1U Serwer
- Interfejsy – 2 x 10/100/1000 Ethernet
- Dwa porty światłowodowe BASE SX, **obsadzone**
- Dwa zasilacze, **redundantne**
- Dwa procesory typu Xeon 2,8 GHz lub równoważne
- Dyski twarde - 2 x 73 GB SCSI DMA 320 Hard Driver RAID 1
- Pamięć 4 GB RAM
- 800 MHz front side bus
- Możliwość montażu w szafie 19”
- Patchcordy światłowodowe do krosowania i podłączenia dla istniejących u Zamawiającego urządzeń oraz sieci,

1.2. Centralny system zarządzania – 2 serwery o minimalnych parametrach pracujące w układzie HA:

Procesor	Architektura x86, L2 1024 MB
Pamięć RAM	4 GB
Grafika	Zintegrowana
Dźwięk	Zintegrowany
Zasilanie	Moc łączna zasilaczy serwera co najmniej 600W
Napęd optyczny	DVD±RW/DVD±R o prędkości nagrywania DVD±R 8x
Obudowa	Dla serwera centralnego – do instalacji w szafie telekomunikacyjnej 19”,
Oprogramowanie	Systemowe - dostosowane do oferowanego rozwiązania, zarządzające, narzędziowe, sterowniki do wszystkich urządzeń, dokumentacja techniczno-instalacyjna

1.3. Oprogramowanie do systemu zarządzania:

1.3.1. Oprogramowanie klastrowe – 1 kpl:

- 2 x VERITAS Storage Foundation Ha 5.0 Windows Standard Edition Std Lic Rewards Band – lub równoważne
- 2 x Database Agent for Microsoft SQL, Windows Advanced/Enterprise Edition,v4.3,License – lub równoważne

1.3.2. Oprogramowanie backupowe - 1 kpl:

- 2xBackup Exec 10d, Windows, Servers with Continuous Protection Server (CPS),v10.1,Multiple License –. lub równoważne
- 2 x Backup Exec 10d, Windows, Microsoft SQL Server Agent with Client Access License and 2 2 x Continuous Protection Agent,v10.1, Multiple License – lub równoważne
- 2 x Backup Exec 10d, Windows, Remote Agent (CAL) for Windows or Netware Servers,v10.1, License – lub równoważne
- 2 x Backup Exec 10d, Windows, Intelligent Disaster Recovery Option Unlimited Clients,v10.1, License – lub równoważne

1.3.3. Dodatkowe oprogramowanie

- Serwer bazy danych Windows SQL Serwer Standard Edition - 1 szt. lub równoważne.

1.4. Szafa typu Rack 19" 42U szt. 1 :

- wysokość użytkowa – 1868 cm
- konsola zarządzająca,
- dwie listwy zasilające, (co najmniej po 5 gniazd 230V/16A na listwie)
- pozostałe parametry szafy muszą być wystarczające do umieszczenia w niej co najmniej 2 szt. serwerów systemu zarządzania i co najmniej 6 urządzeń typu Appliance.

1.5. Stanowisko przenośne do kontroli i zarządzania – 2 szt. o minimalnych parametrach:

Procesor	w architekturze x86 zoptymalizowany do zastosowań mobilnych, 1024 kb L2 cache,
Matryca min.	15,4" XGA display 1680 x 1050
Dysk twardy	min. 80 GB
Pamięć RAM	2 GB
Nagrywarka	DVD±RW/DVD±R o prędkości nagrywania DVD±R min. 4X, obsługa Dual Layer
karta graficzna	128MB z wyjściem SVideo, pamięć karty nie wydzielana z pamięci RAM, przystosowana do zastosowań mobilnych,
Porty zewnętrzne (wbudowane lub poprzez karty)	USB-2.0 – 2 szt, FireWire (IEEE 1394), złącze równoległe, wyjście VGA, interfejsy PC Card typ II lub PC Card typ III, Bluetooth, IrDA, SVideo, WiFi
Waga	Max. 3,0 kg
Czas pracy na baterii	min.2 godz.
Akcesoria	sterowniki do kart (sieciowa, grafika), dokumentacja techniczno – instalacyjna w języku polskim, torba, nośnik pamięci PEN drive 1 GB USB-2., mysz optyczna o rozdzielczości min. 800 dpi, bezprzewodowa, zewnętrzna stacja dysków 3,5" (dołączana poprzez interfejs USB)

Oprogramowanie w języku polskim	Microsoft Windows XP Pro OEM PL lub nowszy + najnowsza stabilna wersja ServicePack (licencja i nośnik CD jeżeli jest), sterowniki do płyty głównej oraz podzespołów komputera dostarczone na oddzielnych nośnikach, Microsoft Office 2003 lub nowszy Pro OEM PL.

1.6. Dostawa, wdrożenie, konfiguracja i instalacja.

1.6.1. Dostawa sprzętu i oprogramowania będzie obejmowała:

a) dostawę urządzeń i oprogramowania do miejsca przeznaczenia lub innego miejsca wskazanego przez Zamawiającego;
b) przygotowanie szczegółowego wykazu sprzętu i oprogramowania

1.6.2. konfiguracja i dokumentacja systemu będzie obejmowała:

a. Opracowanie projektu obejmującego:
   - Reorganizację zasobów pod potrzeby nowego systemu,
   - Sposób włączenia nowych systemów w infrastrukturę Zamawiającego,
   - Instalacje i konfiguracje systemów zarządzania, urządzeń typu Appliance oraz instalacja Agentów ochrony,
b. Opracowanie polityki bezpieczeństwa dla systemu
c. Opracowanie metody backupu systemów.

1.6.3. instalacja urządzeń systemu będzie obejmowała:

a. Instalację urządzeń w miejscu wskazanym przez Zamawiającego;
b. Podłączenie do instalacji elektrycznej;
c. Skrosowanie połączeń;
d. Uruchomienie urządzeń;

1.6.4. Wdrożenie

a. Konfiguracja urządzeń i oprogramowania zgodnie z przyjętym projektem technicznym z uwzględnieniem ciągłości działania krytycznych aplikacji;
b. Strojenie systemów w niezbędnym zakresie;
c. Przeprowadzenie testów;
d. Opracowanie i przekazanie dokumentacji powykonawczej.

1.7. Szkolenia.

Zamawiający wymaga, aby Wykonawca zapewnił i przedstawił do akceptacji Zamawiającego pakiet szkoleń dla grupy administratorów w ilości wystarczającej do sprawnego administrowania i zarządzania oraz samodzielnej obsługi dostarczonych systemów.

Szczegółowe zapisy dotyczące tego zagadnienia zostaną uregulowane w umowie.

2. Zabezpieczenie punktów styku w KWP/KSP.

2.1. Sprzętowe skanery antywirusowe typu Appliance – 34 szt pracujące w układzie HA (High Availability)- w konfiguracji minimalnej:

- **Obudowa – 1U Serwer**
- **Interfejsy – 2 x 10/100/1000 Ethernet**
- **Dwa porty światłowodowe BASE SX, obsadzone**
- **Dwa zasilacze, redundantne**

- **Dwa procesory typu Xeon 2,8 GHz lub równoważne**
- **Dyski twarde - 2 x 73 GB SCSI DMA 320 Hard Driver RAID 1**
- **Pamięć 1 GB RAM**
- **800 MHz front side bus**
- **Możliwość montażu w szafie 19”**
- **Patchcordy światłowodowe do krosowania i podłączenia dla istniejących u Zamawiającego urządzeń oraz sieci,**

Wymagania funkcjonalne dla systemu

1. Minimalne wymagania dla elementów systemu w KGP

1.1. Skaner systemu antywirusowego dla KGP **musi**:

- być dostarczony w formie dedykowanego urządzenia wraz z oprogramowaniem,
- działać na poziomie sieciowym, skanujący protokoły SMTP, POP3, FTP, HTTP
- działać w konfiguracji opartej o protokół ICAP
- działać w trybach Transparent **Bridge**, Transparent Router, Proxy i we wszystkich trybach posiadać taką samą funkcjonalność
- wykrywać i blokować oprogramowanie szpiegujące w protokole HTTP.
- wykrywać próby ataków typu PHISHING
- współpracować z serwerami LDAP pozwalając na stworzenie dokładnej polityki skanowania per email adres lub np. grupa użytkowników w Active Directory
- umożliwiać wysyłanie wiadomości SNMP, syslog oraz powiadomień w formie poczty elektronicznej dla zdefiniowanych zdarzeń
- mieć możliwość **blokady wiadomości typu** spam **oraz** wirus**ów** konkretnego typu (np. Mass Mailery) które zawsze będą usuwane bez powiadamiania użytkowników a wirusy innego typu są standardowo logowane
- wykrywać obecność pakerów **(plików spakowanych)** używanych przez szkodliwe oprogramowanie i musi umożliwiać ich automatyczne skasowanie
- mieć możliwość blokowania wejść na strony które przenoszą złośliwy kod.
- mieć możliwość uruchomienia modułu antyspamowego zarządzanego poprzez wspomniany wyżej centralny serwer zarządzający lub z poziomu interfejsu.
- działać w oparciu o system oceny bazujący na regułach aktualizowanych przez producenta

1.2. System i jego urządzenia dla KGP muszą:

- posiadać wydajność, co najmniej 100Mb/s przy skanowaniu HTTP/FTP lub 210 tysięcy przesyłek SMTP na godzinę.
- umożliwiać budowę centralnej kwarantanny obsługiwanej przez administratora lub bezpośrednio przez użytkowników poprzez przeglądarkę a instalowaną na zewnętrznym serwerze.
- zapewniać możliwość konfiguracji w trybie wysokiej niezawodności oraz skalowania wydajności.
- mieć możliwość monitorowania z wykorzystaniem SNMP.
- obsługiwać białe i czarne listy definiowane przez administratora oraz przez końcowych użytkowników
- oprócz aktualizacji producenta musi wykorzystywać filtry bayesowskie aktualizowane bezpośrednio przez użytkowników systemu.
- **musi być centralnie zarządzany z poziomu KGP**

2. Minimalne wymagania dla elementów systemu w KWP/KSP

2.1. Skaner systemu antywirusowego dla KWP/KSP **musi**:

- być dostarczony w formie dedykowanego urządzenia wraz z oprogramowaniem,
- działać na poziomie sieciowym, skanujący protokoły SMTP, POP3, FTP, HTTP
- działać w konfiguracji opartej o protokół ICAP
- działać w trybach Transparent **Bridge**, Transparent Router, Proxy i we wszystkich trybach posiadać taką samą funkcjonalność
- wykrywać i blokować oprogramowanie szpiegujące w protokole HTTP.
- wykrywać próby ataków typu PHISHING
- współpracować z serwerami LDAP pozwalając na stworzenie dokładnej polityki skanowania per email adres lub np. grupa użytkowników w Active Directory
- umożliwiać wysyłanie wiadomości SNMP, syslog oraz powiadomień w formie poczty elektronicznej dla zdefiniowanych zdarzeń
- mieć możliwość **blokady wiadomości typu** spam **oraz** wirus**ów** konkretnego typu (np. Mass Mailery) które zawsze będą usuwane bez powiadamiania użytkowników a wirusy innego typu są standardowo logowane
- wykrywać obecność pakerów **(plików spakowanych)** używanych przez szkodliwe oprogramowanie i musi umożliwiać ich automatyczne skasowanie
- mieć możliwość blokowania wejść na strony które przenoszą złośliwy kod.
- mieć możliwość uruchomienia modułu antyspamowego zarządzanego poprzez wspomniany wyżej centralny serwer zarządzający lub z poziomu interfejsu.
- działać w oparciu o system oceny bazujący na regułach aktualizowanych przez producenta

2.2. System i jego urządzenia dla KWP/KSP muszą:

- posiadać wydajność, co najmniej 50 Mb/s przy skanowaniu HTTP/FTP lub 120 tysięcy przesyłek SMTP na godzinę.
- umożliwiać budowę centralnej kwarantanny obsługiwanej przez administratora lub bezpośrednio przez użytkowników poprzez przeglądarkę a instalowaną na zewnętrznym serwerze.
- zapewniać możliwość konfiguracji w trybie wysokiej niezawodności oraz skalowania wydajności.
- mieć możliwość monitorowania z wykorzystaniem SNMP.
- obsługiwać białe i czarne listy definiowane przez administratora oraz przez końcowych użytkowników
- oprócz aktualizacji producenta musi wykorzystywać filtry bayesowskie aktualizowane bezpośrednio przez użytkowników systemu.
- **musi być centralnie zarządzany z poziomu KGP**

Załącznik nr 3

WYMAGANIA GWARANCYJNE I SERWISOWE

1. Okres gwarancji – nie krótszy niż 12 miesięcy dla oferowanych urządzeń i oprogramowania **liczone od dnia podpisania protokołu odbioru** dostawy/usługi.
2. Serwis gwarancyjny powinien być oparty na świadczeniach gwarancyjnych producenta sprzętu, niezależnych od statusu partnerskiego dostawcy.
3. Zagłoszenia napraw serwisowych będą dokonywane na podstawie formularza zgłoszeń, którego wzór zostanie uzgodniony przez strony i będzie stanowił załącznik do umowy.
4. Do dostarczonego sprzętu będą dołączone karty gwarancyjne zawierające numery seryjne urządzeń i podzespołów/modułów, termin i warunki ważności gwarancji, adresy i numery telefonów punktów serwisowych świadczących usługi gwarancyjne.
5. W okresie gwarancji Wykonawca zapewni:
   - stały kontakt w celu udzielania konsultacji i pomocy technicznej (w tym również w zakresie systemu operacyjnego) w dni robocze w godz. 8.15 – 16.15,
   - dostarczanie nowych wersji oprogramowania oraz publikowanych poprawek, w czasie trwania Umowy serwisowej wraz z ich instalacją,
6. Pojęcie awarii obejmuje awarię sprzętową i/lub awarię systemu operacyjnego uniemożliwiającą dalsze poprawne działanie sprzętu.
7. Przez usunięcie awarii należy rozumieć przywrócenie pierwotnej funkcjonalności systemu we wszystkich modułach i zaprzestaniu stosowania przez obsługę w bieżącej pracy rezerwowego sprzętu i/lub zastępczych procedur.
8. Po usunięciu każdej awarii, Wykonawca zobowiązuje się do doprowadzenia całego systemu do stanu integralnej całości w rozumieniu poprawnego działania wszystkich zainstalowanych komponentów.
9. Zgłoszenia o awariach będą przyjmowane przez 24 godz. na dobę, przez 7 dni w tygodniu.
10. Wykonawca przystąpi do usunięcia awarii w siedzibie końcowego użytkownika KGP/KWP/KSP w terminie 4 godz. od momentu zgłoszenia awarii drogą telefoniczną, faksową lub e-mail do siedziby serwisu.
11. Naprawa musi nastąpić w ciągu 24 godzin od czasu zgłoszenia. W przypadku braku możliwości naprawy w w/w czasie uszkodzony sprzęt musi zostać zastąpiony równoważnym (sprzęt zastępczy) na czas nie dłuższy niż 90 dni kalendarzowych.
12. Zamawiający nie ponosi żadnych dodatkowych kosztów wynikających z realizacji umowy. Niezbędne komponenty systemu wymieniane będą nieodpłatnie w ramach świadczenia usługi objętej umową i przejdą na własność Zamawiającego.
13. Wykonawca musi zapewnić pełną dokumentację standardowo dostarczoną przez producentów - dokumentacja ta dostarczona będzie w języku polskim lub angielskim.
14. Zamawiający nie zwraca uszkodzonych dysków twardych, w przypadku wymiany uszkodzonego na nowy.
15. Dyski zastępcze dostarczone na czas naprawy podlegają skasowaniu wg procedury opisanej w wytycznych Departamentu Bezpieczeństwa Teleinformacyjnego ABW.
16. Wykonawca określi zakres i charakter modyfikacji, które może wykonać Zamawiający w czasie eksploatacji sprzętu bez naruszenia warunków umowy.
17. W trakcie trwania gwarancji Oferent musi zapewnić wsparcie techniczne dla dostarczonych systemów obejmujące minimum następujące elementy:

- dostarczanie nowych wersji oprogramowania,
- wsparcie techniczne przez certyfikowanych inżynierów świadczone telefoniczne oraz poprzez e-mail,