Miejski Ośrodek Pomocy Społecznej w Krakowie

30-529 Kraków, ul. Józefińska 14, tel. +4812 616 54 27, fax. +4812 616 54 28-mail: sz@poczta.mops.krakow.pl

SZ.271.1.1421.2015

Kraków, dnia 20. 11. 2015

Ogłoszenie w sprawie zamówienia publicznego udzielanego w trybie do 30 000 euro.

Podstawa prawna zastosowania trybu: art. 4 pkt. 8 ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych (jt.: Dz. U. z 2013 roku, poz. 907 z późniejszymi zmianami)

Opis przedmiotu zamówienia:

1. Przedmiotem zamówienia jest:
   1.1. Zakup sprzętu informatycznego - serwera bezpieczeństwa sieciowego firewall typu appliance (urządzenie + oprogramowanie) – **Fortigate 200D** - 1 szt.
   1.2. Zakup sprzętu informatycznego – serwera sieciowego do zapisywania zdarzeń i raportowania umożliwiające zarządzanie wszystkimi funkcjonalnościami elementów realizujących funkcję bezpieczeństwa w ramach całej infrastruktury zabezpieczeń Zamawiającego. – **FortiAnalyzer 200D** – 1 szt.
   1.3. Zakup serwera sieciowego zapewniającego kompleksową ochronę antyspamową, antywirusową i antyspyware'ową dla serwera poczty zamawiającego – **FortiMail VM01** – 1 szt.
   1.4. Uruchomienie, wdrożenie oraz szkolenia dot. serwerów, o których mowa w pkt. 1.1 do 1.3
2. Szczegółowe wymagania ogólne oraz techniczne dla urządzenia wymienionego w pkt. 1.1:
   2.1. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
   2.2. Możliwość łączenia w klaster Active-Active lub Active-Passive każdego z elementów systemu.
   2.3. Elementy systemu przenoszące ruch użytkowników powinny dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub Bridge/transparent.
   2.4. Urządzenie musi posiadać minimum 16 szt. interfejsów Ethernet 10/100/1000 Base-TX pracującymi niezależnie oraz 2 gniazdami SFP 1Gbps.
   2.5. System musi umożliwiać zdefiniowanie co najmniej 254 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
   2.6. Monitoring stanu realizowanych połączeń VPN.
   2.7. Urządzenie musi posiadać lokalny dysk twardy o pojemności min. 50GB do celów logowania i raportowania.
   2.8. W zakresie Firewall'a obsługa nie mniej niż 3 miliony jednoczesnych połączeń oraz nie mniej niż 70 tys. nowych połączeń na sekundę.
   2.9. Przepustowość Firewall'a: nie mniej niż 3 Gbps dla pakietów 512 B
   2.10. Wydajność szyfrowania VPN IPSec: nie mniej niż 1,2 Gbps
   2.11. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych:
   - Kontrola dostępu - zapora ogniowa klasy Stateful Inspection

- Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS
- Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN
- Ochrona przed atakami - Intrusion Prevention System
- Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
- Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP
- Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma
- Kontrola aplikacji – system musi rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów)
- Możliwość analizy ruchu szyfrowanego protokołem SSL
- Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)

2.12. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych.

2.13. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 1,7 Gbps

2.14. Wydajność skanowania ruchu z włączoną funkcją Antywirus - minimum 600 Mbps

2.15. W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż:

- Tworzenie połączeń w topologii Site-to-site oraz Client-to-site
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
- Praca w topologii Hub and Spoke oraz Mesh
- Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF
- Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth

2.16. W ramach funkcji IPSec VPN, SSL VPN – producent musi dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.

2.17. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

2.18. Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSec VPN'a Antywirus'a, IPS'a.

2.19. Translacja adresów NAT adresu źródłowego i docelowego.

2.20. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.

2.21. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ

2.22. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)

2.23. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 4500 wpisów. Ponadto administrator systemu musi mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.

2.24. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP

2.25. Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator musi mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW.

2.26. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.

2.27. System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż:

- Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
- haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
- haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych
- Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu „Single Sign On" w środowisku Microsoft Active Directory

2.28. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:

1) ICSA lub EAL4 dla funkcji Firewall
2) ICSA lub NSS Labs dla funkcji IPS
3) ICSA dla funkcji: SSL VPN, IPSec VPN

2.29. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

2.30. System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze lub do lokalnego serwera logów w zakresie logowania i raportowania w postaci odpowiednio zabezpieczonej platformy sprzętowej lub programowej.

2.31. Serwisy i licencje:

1) W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres 2 lat.
2) System musi być objęty standardowym serwisem gwarancyjnym producenta przez okres 24 miesięcy, realizowanym na terenie Rzeczypospolitej Polskiej, umożliwiającym wymianę wadliwego urządzenia do 14 dni.
3) System musi być objęty dodatkowym serwisem gwarancyjnym producenta przez okres 12 miesięcy umożliwiającym wymianę wadliwego urządzenia w następnym dniu roboczym.
4) W przypadku, gdy producent nie posiada na terenie Rzeczypospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczypospolitej Polskiej.

3. Szczegółowe wymagania ogólne oraz techniczne dla urządzenia wymienionego w pkt. 1.2:
   3.1. W ramach systemu logowania i raportowania dostawca musi dostarczyć spójny system monitorujący, gromadzący logi, korelujący zdarzenia i generujący raporty na podstawie danych ze wszystkich elementów systemu bezpieczeństwa objętych tym zamówieniem.
   3.2. Platforma powinna dysponować predefiniowanym zestawem przykładów raportów, dla których administrator systemu będzie mógł modyfikować parametry prezentowania wyników.
   3.3. System centralnego logowania i raportowania musi być dostarczony w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
   3.4. Konfigurowalne opcje powiadamiania o zdarzeniach jak. email, SNMP
   3.5. Podgląd logowanych zdarzeń w czasie rzeczywistym.
   3.6. Możliwość generowania raportów w zakresie wszystkich funkcjonalności bezpieczeństwa realizowanych przez system - na żądanie oraz w trybie cyklicznym, w postaci popularnych formatów min: PDF, DOC, HTML. Raporty powinny obejmować zagadnienie dotyczące całej sfery bezpieczeństwa.
   3.7. Zastosowane systemy logowania powinny umożliwiać cykliczny eksport zgromadzonych logów do zewnętrznych systemów przechowywania danych w celu ich długo czasowego składowania.
   3.8. Na podstawie analizy przeprowadzonych testów w zakresie ilości logów w ciągu sekundy, zastosowany system centralnego logowania musi umożliwiać zapis oraz analizę co najmniej 120 nowych logów/sekundę.
   3.9. System musi dysponować co najmniej 4 interfejsami Ethernet 10/100/1000 oraz powierzchnią dyskową min. 1 TB.
   3.10. Serwisy i licencje
   1) System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, realizowanym na terenie Rzeczypospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w ciągu 14 dni.
   2) W przypadku gdy producent nie posiada na terenie Rzeczypospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczypospolitej Polskiej.
4. Szczegółowe wymagania ogólne oraz techniczne dla urządzenia wymienionego w pkt. 1.3:
   4.1. Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia.
   4.2. System musi być dostarczony w postaci komercyjnej platformy działającej w środowisku wirtualnym z możliwością uruchomienia na Hyper-V 2008R2, Hyper-V 2012 lub Hyper-V 2012R2.
   4.3. System musi zapewniać obsługę nie mniej niż 4 interfejsów Ethernet 10/100/1000 Base-TX
   4.4. System musi zapewniać powierzchnia dyskowa - minimum 1 TB.

4.5. System musi zapewniać możliwość dołączenia dodatkowych urządzeń blokowych bez ograniczeń powierzchni dyskowych m.in. poprzez protokół iSCSI.
4.6. System musi zapewniać obsługę nie mniej niż 50 profili antywirusowych lub antyspamowych.
4.7. System musi zapewniać wydajność min. 20.000 wiadomości/godzinę.
4.8. Urządzenie powinno mieć możliwość pracy w każdym z trzech trybów:
1) Tryb gateway
2) Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej)
3) Tryb serwera pocztowego
4.9. System musi realizować poniższe funkcjonalności w każdym z trzech trybów pracy ujętych w pkt 4.6:
1) Wsparcie dla wielu domen pocztowych min. 20
2) Polityki filtrowania tworzone w oparciu o adresy mailowe, nazwy domenowe, adresy IP (w szczególności reguła all-all)
3) Email routing oraz zarządzanie kolejkami bazujące na politykach
4) Ochrona poczty przychodzącej oraz wychodzącej
5) Granularne, wielowarstwowe polityki wykrywania spamu oraz wirusów
6) Skanowanie Antywirusowe oraz Antyspamowe definiowane na użytkownika w oparciu o atrybuty LDAP
7) Routing poczty (email routing) w oparciu o LDAP
8) Kwarantanna poczty z dziennym podsumowaniem (możliwość samodzielnego zwalniania plików z kwarantanny przez użytkownika)
9) Dostęp do kwarantanny poprzez WebMail lub POP3
10) Archiwizacja poczty przychodzącej i wychodzącej, backup poczty do różnych miejsc przeznaczenia
11) Uwierzytelnianie SMTP w oparciu o protokoły: LDAP, RADIUS, POP3, IMAP
12) Mechanizmy reputacji nadawcy wiadomości
13) Whitelist'y definiowane dla użytkownika
4.10. System musi realizować poniższe funkcjonalności w trybie serwera pocztowego:
1) Obsługa minimum 100 lokalnych skrzynek pocztowych
2) Obsługę serwisów pocztowych: SMTP, POP3, IMAP
3) Wsparcie SMTP over SSL
4) Definiowanie powierzchni dyskowej dla użytkowników
5) Szyfrowany dostęp do poczty poprzez WebMail
6) Polski interfejs użytkownika przy dostępie przez WebMail
7) Kalendarz na WebMail'u
8) Lokalne konta użytkowników oraz uwierzytelnianie w oparciu o LDAP
9) Synchronizacja książki adresowej z LDAP
4.11. System musi realizować skanowanie antywirusowe wiadomości SMTP.
4.12. System musi realizować kwarantannę dla zainfekowanych plików.
4.13. System musi realizować skanowanie załączników skompresowanych (w tym 7z, bzip2, jar, zipx, rar, arj).
4.14. System musi realizować możliwość definiowania komunikatów powiadomień w języku polskim.

40

4.15. System musi realizować blokowanie załączników ze względu na typ pliku.
4.16. System musi zapewniać poniższe metody filtrowania spamu:
1) Heurystyczna analiza poczty z dynamiczną aktualizacją reguł
2) Filtrowanie treści załączników, filtrowanie wiadomości po słowach kluczowych
3) Szczegółowa kontrola nagłówka wiadomości
4) Filtrowanie w oparciu o filtry Bayes'a, z możliwością dostrajania dla poszczególnych użytkowników
5) Filtrowanie poczty w oparciu o sumy kontrolne spamu
6) Wykrywanie spamu w oparciu a analizę plików graficznych oraz plików PDF
7) Analiza poczty w oparciu o dynamiczną bazę spamu dostarczaną przez tego samego producenta
8) Współpraca z zewnętrznymi serwerami RBL
9) Kontrola w oparciu o Greylist'y
10) Białe i czarne listy definiowane globalnie oraz per użytkownik
11) Weryfikacja źródłowego adresu IP
12) Mechanizmy reputacji użytkownika
13) Możliwe akcje dla poczty: Accept, Relay, Reject,, Discard, Kwarnatanna, Oznaczanie (Tagging)

4.17. System musi zapewniać ochronę przed atakami DoS:
1) Denial of Service (Mail Bombing)
2) Ochrona przed atakami na adres odbiorcy
3) Definiowanie maksymalnych ilości wiadomości pocztowych
4) Kontrola Reverse DNS (Anty-Spoofing)
5) Weryfikacja poprawności adresu e-mail nadawcy

4.18. 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.
4.19. System musi zapewniać mechanizmy wsparcia dla szyfrowanych protokołów: HTTPS, SMTPS, IMAPS, POP3S
4.20. System musi zapewnić możliwość logowania SNMP dla zdarzeń systemowych z możliwością definiowania progów oraz logowanie do zewnętrznego serwera SYSLOG
4.21. System musi zapewnić możliwość logowania zmian konfiguracji, krytycznych zdarzeń systemowych, działalności wirusów, spamu oraz niedozwolonych załączników.
4.22. System musi posiadać predefiniowane szablony raportów oraz planowania czasu generowania raportów na ich podstawie.
4.23. System musi umożliwiać podgląd logów w czasie rzeczywistym.
4.24. System musi umożliwiać archiwizację poczty w oparciu o zestaw filtrów.
4.25. System musi zapewniać konfigurację HA w konfiguracji:
1) Active-Passive w każdym z trybów: gateway, transparent, serwer,
2) Active-Passive z syncronizacją polityk i wiadomości, gdzie cluster występuje pod jednym adresem IP
3) synchronizacji konfiguracji dla scenariuszy rozległych (osobne adresy IP)

4.26. Konfiguracja HA musi zapewniać funkcjonalność wykrywania awarii i powiadamiania administratora oraz monitorowania stanu połączeń.

4.27. System musi zapewniać pracę w oparciu o bazę spamu uaktualnianą w czasie rzeczywistym, planowanie aktualizacji szczepionek antywirusowych w czasie (Scheduler) oraz możliwość wymuszenia aktualizacji bazy wirusów (tryb push).

4.28. System musi umożliwiać zarządzanie poprzez szyfrowane połączenia HTTPS oraz SSH.

4.29. Serwisy i licencje:

1) W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz spamu, definicji wirusów i innych zabezpieczeń przez okres 2 lat.
2) System musi być objęty standardowym serwisem gwarancyjnym producenta przez okres 24 miesięcy, realizowanym na terenie Rzeczypospolitej Polskiej, umożliwiającym wymianę wadliwego systemu do 14 dni.
3) W przypadku gdy producent nie posiada na terenie Rzeczypospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczypospolitej Polskiej.

5. Szczegółowe wymagania dotyczące usługi uruchomienia, wdrożenia oraz szkoleń z pkt. 1.4:

5.1. Wykonawca uruchomi wdroży oraz przeszkoli 2 administratorów w terminie nie późniejszym niż do dnia 22 grudnia 2015 roku.

5.2. Czynności wymienione w pkt. 5.1 Wykonawca zapewni w siedzibie zamawiającego przy ul. Józefińskiej 14 w Krakowie.

5.3. Dla czynności wymienionych w pkt. 5.1 wykonawca zapewni minimum 60 godzin roboczych w godzinach pracy zamawiającego, tj. od poniedziałku do piątku w godz. 07:30-15:30, przy czym rozpoczęcie prac wdrożeniowych rozpocznie się nie później niż w dniu 7 grudnia 2015 roku.

5.4. Dla serwerów wymienionych w pkt. 1.1 do 1.3 wykonawca zapewni dokumentacje techniczną w języku polskim (dopuszczalna jest dokumentacja w formacie elektronicznym).

Warunki realizacji zamówienia zostały określone we wzorze umowy, załączonym do niniejszego ogłoszenia. Zamawiający nie dopuszcza możliwości składania ofert częściowych.

Oferty na formularzu ofertowym sporządzonym wg wzoru stanowiącego załącznik do niniejszego ogłoszenia należy składać na adres mailowy: sz@mops.krakow.pl **w terminie do dnia 25 listopada 2015 roku do godziny 10:00**. W tytule wiadomości proszę wpisać *„Oferta dotycząca zamówienia nr 271.1.1421.2015”.*

Oferta, złożona w języku polskim, powinna zawierać:

1. Nazwę i dokładny adres Wykonawcy,
2. Datę sporządzenia oferty,
3. Ceny jednostkowe netto i brutto.
4. Pełnomocnictwo dla osoby podpisującej ofertę, jeżeli nie jest ona uprawniona do reprezentowania podmiotu, zgodnie z wypisem z Krajowego Rejestru Sądowego lub Centralnej Ewidencji i Informacji o Działalności Gospodarczej.

Zamawiający będzie oceniał oferty według następującego kryterium cena = 100%

$$\text{kryterium ceny} = \frac{\text{cena najniższa brutto spośród ważnych ofert}}{\text{cena brutto badanej oferty}} \times 100\%$$

Oferta, która przedstawia najkorzystniejszy bilans (maksymalna liczba przyznanych punktów w oparciu o ustalone kryteria) zostanie uznana za najkorzystniejszą. Realizacja zamówienia zostanie powierzona wykonawcy, którego oferta uzyska najwyższą liczbę punktów.

z upoważnienia Dyrektora
Wioletta Zielińska
Kierownik
Sekcji Zamówień Publicznych

Załączniki:

1. Formularz ofertowy,
2. Wzór umowy.

Inspektor
Tomasz Stefański

Kierownik Sekcji Informatyzacji
Maciej Stefaniczyk
15.12.2015

Załącznik do Ogłoszenia w sprawie zamówienia publicznego udzielanego w trybie do 30 000 euro.

(pieczęć adresowa Wykonawcy)

Miejski Ośrodek Pomocy Społecznej
ul. Józefińska 14
30-529 Kraków

OFERTA
do zamówienia nr ZP 271.1.1421.2015

W odpowiedzi na ogłoszenie wszczęcia postępowania o udzielenie zamówienia publicznego na dostawę serwerów dla Miejskiego Ośrodka Pomocy Społecznej w Krakowie oraz uruchomienie, wdrożenie i szkolenie personelu Zamawiającego składam niniejszą ofertę. Oferuję wykonanie przedmiotu zamówienia za cenę ..... zł netto, tj. ..... zł brutto *(określoną z dokładnością do dwóch miejsc po przecinku)*, z czego za:

1. serwer bezpieczeństwa sieciowego firewall typu appliance (urządzenie + oprogramowanie) – Fortigate 200D ..... zł netto, tj. ..... zł brutto;
2. serwer sieciowy FortiAnalyzer 200D ..... zł netto, tj. ..... zł brutto;
3. serwer sieciowy FortiMail VM01 ..... zł netto, tj. ..... zł brutto;
4. uruchomienie, wdrożenie oraz szkolenie ..... zł netto, tj. ..... zł brutto.

Okresy gwarancji:

1. serwer bezpieczeństwa sieciowego firewall typu appliance (urządzenie + oprogramowanie) – Fortigate 200D ..... miesięcy;
2. serwer sieciowy FortiAnalyzer 200D ..... miesięcy;
3. serwer sieciowy FortiMail VM01 ..... miesięcy;
4. uruchomienie, wdrożenie oraz szkolenie ..... miesięcy.

<u>Oświadczam, że:</u>

1. Cena oferty uwzględnia wszystkie koszty wykonania przyszłego świadczenia umownego.
2. Zapoznałem się z treścią Ogłoszenia w sprawie zamówienia publicznego udzielanego w trybie do 30 000 euro, uznaję się za związanego określonymi w nim postanowieniami i zobowiązuję się - w przypadku wyboru mojej oferty - do zawarcia umowy zgodnej z wzorem stanowiącym załącznik do ogłoszenia, na warunkach wynikających z niniejszej oferty i ogłoszenia w terminie zaproponowanym przez Zamawiającego.
3. Akceptuję warunki realizacji zamówienia określone przez Zamawiającego we wzorze umowy, stanowiącym załącznik do Ogłoszenia w sprawie zamówienia publicznego udzielanego w trybie do 30 000 euro.

4. Zamówienie zrealizuję samodzielnie (przy udziale podwykonawców)[1]

   1. .....
   (zakres podzlecanej usługi i jej wartość)

   2. .....
   (zakres podzlecanej usługi i jej wartość)

5. Za wyjątkiem informacji i dokumentów zawartych na stronach ..... niniejsza oferta wraz z załącznikami do niej jest jawna i nie zawiera informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji.

Wszelką korespondencję w sprawie niniejszego postępowania należy kierować pod adres oferenta:
.....

nr telefonu/faksu.....

adres mailowy: .....

Numer rachunku bankowego: .....

Oferta niniejsza zawiera ..... kolejno ponumerowanych i podpisanych przez osobę upoważnioną stron.
Integralną część oferty stanowią niżej wymienione załączniki:

1. ..... (proszę wymienić jakie)

....., dnia .....
(miejscowość)

.....
(podpis wykonawcy)

z upoważnienia Dyrektora
Wielkopolskiego
Ośrodka
Doradztwa
Sekcja Zamówień Publicznych

[1] Niewłaściwe skreślić

Umowa (wzór)

Zawarta w dniu ..... w Krakowie pomiędzy:
Miejskim Ośrodkiem Pomocy Społecznej w Krakowie, 30-529 Kraków, ul. Józefińska 14, NIP 677-17-34-298, REGON 351505308, reprezentowanym przez ....., zwanym dalej *„Zamawiającym"*
a
..... z siedzibą w ....., nr NIP ....., nr REGON ....., reprezentowanym przez ....., zwanym w dalszej części *„Wykonawcą"*, łącznie zwanymi *„Stronami"* o następującej treści:

§1

Umowa zostaje zawarta w wyniku przeprowadzenia postępowania o udzielenie zamówienia publicznego w trybie, do którego, zgodnie z dyspozycją art. 4 pkt. 8 ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2013 roku, poz. 907 z późniejszymi zmianami), nie stosuje się przepisów tej ustawy.

§2

1. Przedmiotem zamówienia jest zakup i dostawa:
   1) serwera bezpieczeństwa sieciowego firewall typu appliance (urządzenie + oprogramowanie) – **Fortigate 200D** - 1 szt,
   2) serwera sieciowego do zapisywania zdarzeń i raportowania umożliwiające zarządzanie wszystkimi funkcjonalnościami elementów realizujących funkcję bezpieczeństwa w ramach całej infrastruktury zabezpieczeń zamawiającego. – **FortiAnalyzer 200D** – 1 szt,
   3) serwera sieciowego zapewniającego kompleksową ochronę antyspamową, antywirusową i antyspyware'ową dla serwera poczty zamawiającego – **FortiMail VM01** – 1 szt

   zwanych w dalszej części „towarem", szczegółowo opisanych w załączniku numer 1 do niniejszej umowy.
2. Przedmiot umowy obejmuje także uruchomienie, wdrożenie oraz szkolenia personelu Zamawiającego dot. serwerów, o których mowa w ust. 1 niniejszego paragrafu.
3. Miejsce dostawy: magazyn centralny Zamawiającego Kraków, ul. Józefińska 14, w godzinach: poniedziałek - piątek 07:30-14:30.
4. Wykonawca dostarczy zamawiany towar własnym transportem i na własny koszt, w sposób zapewniający jego całość i nienaruszalność. Opakowanie i sposób przewozu powinny odpowiadać jego właściwościom.
5. Dostarczony towar będzie fabrycznie nowy, nie będzie nosić śladów użytkowania oraz zostanie dostarczony w oryginalnych, nienaruszonych opakowaniach. Towar będzie kompletny z punktu widzenia celu jakiemu ma służyć i zdatny do bezpośredniego użycia zgodnie z przeznaczeniem.
6. Okres gwarancji jest określony w ofercie Wykonawcy, stanowiącej załącznik numer 2 do niniejszej umowy.
7. Dokumentem udzielenia gwarancji jest niniejsza umowa.
8. Serwis gwarancyjny będzie wykonywany w lokalach, w których będzie zlokalizowany sprzęt komputerowy, na koszt Wykonawcy. W szczególnie uzasadnionych przypadkach naprawy gwarancyjne mogą odbywać się poza lokalami Zamawiającego, jedynie za zgodą Zamawiającego. Lokale mieszczą się na terenie Miasta Krakowa. Naprawy gwarancyjne będą wykonywane w ciągu 4 dni od momentu zgłoszenia awarii (faksem lub e-mailem). Do czasu naprawy nie wlicza się sobót oraz dni świątecznych.

9. Faktura będzie zawierać szczegółowe zestawienie towaru /precyzyjne nazwy wszystkich elementów składowych.
10. Zamawiający nie odbierze towaru w przypadku, gdy Wykonawca przy dostawie nie dostarczy również poprawnie wystawionej faktury.
11. W przypadku stwierdzenia przez Zamawiającego w ciągu 30 dni od dostawy wad lub braków ilościowych w dostarczonym towarze Wykonawca ma obowiązek wymienić wadliwy towar lub uzupełnić brakujący towar do 7 dni od daty otrzymania zgłoszenia.

§3

Strony ustalają następujące terminy realizacji przedmiotu umowy:
1) dostawa towaru do dnia .....,
2) uruchomienie do dnia .....,
3) wdrożenie do dnia .....,
4) szkolenie personelu Zamawiającego do dnia .....

§4

1. Zamawiający zapłaci Wykonawcy za towar cenę łączną nie wyższą niż ..... zł brutto (słownie: ..... złotych 75/100), zgodnie z ofertą Wykonawcy, stanowiącą załącznik numer 2 do niniejszej umowy.
2. Wynagrodzenie zostanie zapłacone przelewem w terminie do 14 dni od daty przyjęcia faktury przez Zamawiającego, na rachunek bankowy Wykonawcy wskazany w fakturze.
3. Wykonawca wystawi fakturę zgodnie z zasadami określonymi w przepisach rozporządzenia Ministra Finansów z dnia 3 grudnia 2013 roku w sprawie wystawiania faktur (Dz. U. z 2013 roku, poz. 1485).Wykonawca wraz z fakturą dostarczy protokół odbioru towaru do magazynu centralnego Zamawiającego w Krakowie przy ul. Józefińskiej 14. Protokół będzie podpisany przez upoważnionego pracownika Zamawiającego w miejscu dostawy.

§5

Odbioru towaru ze strony Zamawiającego dokonają magazynier lub osoba go zastępująca oraz kierownik Sekcji ds. Informatyzacji lub osoba go zastępująca.

§6

1. Wykonawca zapłaci Zamawiającemu karę umowną za:
   1) opóźnienie w dostarczeniu przedmiotu zamówienia w stosunku do terminu określonego w §3 pkt. 1 w wysokości 1% wartości partii towaru dostarczonego z opóźnieniem, za każdy dzień opóźnienia,
   2) opóźnienie w uruchomieniu, wdrożeniu oraz przeszkoleniu personelu Zamawiającego w stosunku do terminów określonych w §3 pkt. 2-4 w wysokości 1% wynagrodzenia umownego, o którym mowa w §4 ust. 1, za każdy dzień opóźnienia,
   3) opóźnienie w usunięciu wad lub braków ilościowych przedmiotu umowy w stosunku do terminu określonego w §2 ust. 11 w wysokości 1% wartości towaru podlegającego reklamacji za każdy dzień opóźnienia,
   4) opóźnienie dokonania naprawy gwarancyjnej w stosunku do terminu określonego w §2 ust. 8 w wysokości 1% wartości ofertowej towaru za każdy dzień opóźnienia,
   5) odstąpienie od umowy z przyczyn leżących po stronie Wykonawcy w wysokości 10% wynagrodzenia umownego, o którym mowa w §4 ust. 1.
2. Wszelkie kary umowne mogą być potrącane z wynagrodzenia należnego Wykonawcy.
3. Zamawiający zastrzega sobie prawo dochodzenia na zasadach ogólnych odszkodowania uzupełniającego, przewyższającego wysokość kary umownej zastrzeżonej w umowie, a także dochodzenia i naliczenia kar umownych, również po odstąpieniu od umowy.

§7

1. W przypadku niewykonania lub nienależytego wykonywania przez Wykonawcę niniejszej umowy, a w szczególności, gdy: Wykonawca dostarczy towar o parametrach gorszych od zadeklarowanych w ofercie lub noszący ślady używania, przeróbek, nieoryginalnie zapakowany, uszkodzony, niezdatny do umówionego użytku Zamawiający zastrzega sobie prawo odstąpienia od umowy z przyczyn leżących po stronie Wykonawcy w terminie 30 dni od dnia wystąpienia okoliczności uzasadniających skorzystanie przez Zamawiającego z prawa odstąpienia od umowy.
2. Odstąpienie od umowy powinno nastąpić wyłącznie w formie pisemnej pod rygorem nieważności i winno zawierać uzasadnienie.

§8

1. Zmiany umowy wymagają formy pisemnej.
2. Zamawiający dopuszcza zmianę treści niniejszej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy w następującym zakresie: wydłużenia okresu gwarancji; miejsca i godzin dostawy towaru; warunków płatności.
3. Zmiana umowy dokonana z naruszeniem powyższych postanowień jest nieważna.

§9

W sprawach nie uregulowanych niniejszą umową mają zastosowanie przepisy ustawy z dnia 23 kwietnia 1964 roku Kodeks cywilny (tekst jednolity: Dz. U. z 2014 roku, poz. 121 z późniejszymi zmianami) oraz ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2013 roku, poz. 907 z późniejszymi zmianami)

§10

Zamawiający oświadcza, że nie wyraża zgody na cesję wierzytelności wynikających z umowy.

§11

1. Przed wystąpieniem na drogę sądową Strony ustalają obligatoryjny tryb postępowania polubownego, polegający w szczególności na konieczności sprecyzowania zarzutów wobec drugiej Strony na piśmie. Druga Strona ma obowiązek udzielenia pisemnej odpowiedzi na pisemne zarzuty Strony. Brak odpowiedzi, w terminie 14 dni lub odmowa udzielenia odpowiedzi daje podstawę do wystąpienia na drogę sądową.
2. Spory mogące wyniknąć w trakcie wykonywania umowy strony podają rozstrzygnięciu sądu właściwego dla siedziby Zamawiającego.

§12

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla Wykonawcy i Zamawiającego.

Za Wykonawcę

.....

Za Zamawiającego:

.....

Kierownik Sekcji Informatyzacji
Maciej Stefańczyk
13.11.2015

Monika Małgorzata Senior-Czarnota
WR-1197
20.11.15