Szczegółowy opis przedmiotu zamówienia – Część II

Przedmiotem zamówienia – dla Części II - jest przedłużenie gwarancji, licencji na aktualizację oprogramowania oraz wsparcia technicznego producenta dla poniżej wymienionych systemów bezpieczeństwa teleinformatycznego Zamawiającego:

1) dodatkowa, na okres zgodny z ofertą Wykonawcy, ale nie krócej niż 24 miesiące, subskrypcja wsparcia producenta na licencje aktywacyjne dla wszystkich funkcji bezpieczeństwa systemu dwuskładnikowego uwierzytelniania użytkowników Zamawiającego: **FortiAuthenticator VM**. Dotychczasowa subskrypcja wygasa w dniu 08.04.2016 r.;
2) dodatkowy, przedłużający na okres zgodny z ofertą Wykonawcy, ale nie krócej niż 24 miesiące, serwis gwarancyjny i wsparcie producenta, realizowane na terenie Rzeczypospolitej Polskiej, polegające na naprawie lub wymianie urządzenia w przypadku jego wadliwości w terminie 14 dni roboczych od daty zgłoszenia serwisowego oraz dodatkowe, na okres zgodny z ofertą Wykonawcy, ale nie krótsze niż 24-miesięczne licencje aktywacyjne dla wszystkich funkcji bezpieczeństwa dla systemu ochrony sieci VPN Zamawiającego: **FortiGate 90D (17 sztuk)**. Dotychczasowy serwis gwarancyjny i wsparcie producenta wygasa w dniu 05.11.2016 r.;
3) Wykonawca zobowiązany jest załączyć do oferty oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży przedłużania gwarancji, licencji na aktualizację oprogramowania oraz wsparcia technicznego oraz świadczenia usług z nimi związanych;
4) przed zawarciem umowy w sprawie zamówienia publicznego, Wykonawca zobowiązany jest dostarczyć Zamawiającemu oświadczenie producenta lub autoryzowanego dystrybutora producenta informujące o możliwości przyjęcia uszkodzonego urządzenia objętego serwisem do naprawy u dystrybutora na terenie Polski;
5) serwis, o którym mowa w pkt 4, musi być realizowany przez Producenta rozwiązania lub Autoryzowanego Dystrybutora Producenta, mającego swoją lokalizację serwisową na terenie Polski, posiadającego certyfikat ISO 9001 w zakresie usług serwisowych (należy dołączyć go do oferty);
6) Wykonawca zobowiązany jest zapewnić pierwszą linię wsparcia technicznego, telefonicznie lub poprzez e-mail, w języku polskim w trybie 8 godzin od 9:00 do 17:00, 5 dni w tygodniu (poniedziałek-piątek) przez okres wskazany w ofercie Wykonawcy, ale nie krócej niż 24 miesięce;

7) w przypadku, gdy producent nie posiada na terenie Rzeczypospolitej Polskiej własnego centrum serwisowego, Wykonawca powinien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczypospolitej Polskiej. Zamawiający wymaga, aby dokument ten, Wykonawca przedłożył przed zawarciem umowy w sprawie zamówienia publicznego.

Integralną częścią zakupu usługi wsparcia technicznego dla urządzeń sieciowych będzie przeszkolenie 3 pracowników wskazanych przez Zamawiającego z zakresu implementacji i administrowania ustawieniami zabezpieczeń w środowiskach Windows Client (7/8.1/10) oraz Windows Server (2008R2/2012R2/2016). Szkolenie musi obejmować następującą tematykę:

1) Modele zarządzania infrastrukturą IT;
2) Zarządzanie bezpieczeństwem i zgodnością ze standardami;
3) Linia odniesienia dla ról i funkcji Windows Server;
4) Poziomy ważności i reguły zabezpieczeń;
5) Strategia bezpieczeństwa Defense in depth;
6) Zagadnienia bezpieczeństwa rodziny Windows Client & Windows Server;
7) Narzędzia oceny:
   a) Microsoft Assessment Tool,
   b) Microsoft Baseline Security Analyzer,
   c) Microsoft Security Compliance Manager,
   d) Microsoft Message Analyzer;
8) Technologie ochrony:
   a) Konsola Action Center,
   b) Listy kontroli dostępu (ACL),
   c) Dynamiczna kontrola dostępu (DAC),
   d) Polityki kontroli i audytów (Audit Policies),
   e) Kontrola, zarządzanie i archiwizacja zdarzeń systemowych,
   f) Centralizacja zarządzania zdarzeniami systemowymi (Event Forwarding),
   g) Prawa użytkowników (User Rights),
   h) Stosowanie grup wbudowanych i tożsamości specjalnych,
   i) Polityki haseł granularnych (PSO) oraz grupy typu Shadow,
   j) Opcje bezpieczeństwa systemu (Security Options),
   k) Ustawienia usług systemowych,
   l) Ograniczanie uruchamiania aplikacji za pomocą AppLocker,

m) Konfiguracja i stosowanie IPSec oraz reguł zabezpieczania ruchu sieciowego (Connection Security Rules),
n) Konfiguracja i monitorowanie Windows Firewall oraz zaawansowanych ustawień reguł zapory,
o) Szyfrowanie Bitlocker oraz Bitlocker To Go,
p) Zarządzanie Trusted Platform Module (TPM),
q) Szyfrowanie Encrypted File System,
r) Konfiguracja menedżera poświadczeń,
s) Konta usługowe,
t) Konfiguracja Secure Boot,
u) Zastosowanie Security Configuration Wizard (SCW),
v) Konfiguracja kontroli konta użytkownika (User Account Control),
w) Ograniczenie podatności na ataki za pomocą EMET,
x) Ograniczenie dostępu do urzadzeń (np. USB),
y) Centralizacja danych użytkownika z zastosowaniem przekierowania folderów (Folde Redirection) i ich klasyfikacja (File Classifiation Infrastructure),
z) Wykorzystanie Active Directory Rights Management Services w ochronie dostępu do danych,
aa) Konfiguracja i zastosowanie Internet Explorer Enterprise Mode,
bb) Konfiguracja i monitorowanie oprogramowania antywirusowego oraz zapobiegającem wykonywania złośliwego oprogramowania Microsoft Security Essential,
cc) Preferencje i ustawienia zabezpieczeń;

9) Narzędzia administracyjne:
a) dostęp do zasobów,
b) rejestrowanie dostępu,
c) zadania związane z urzędem certyfikatów CA,
d) zarządzanie procesami oraz wydajnością,
e) zarządzanie poświadczeniami obiektów,
f) zarządzanie certyfikatami i szyfrowaniem,
g) właściciele obiektów oraz pełne usuwanie danych,
h) polityki kontroli oraz zarządzanie zdarzeniami,
i) polityki zabezpieczania systemu,
j) diagnostyka, planowanie i poprawianie ustawień;

10) Ustawienia zabezpieczeń w środowisku domeny;
11) Zarządzanie ustawieniami zabezpieczeń w modelu hybrydowym.

Szkolenie musi zostać przeprowadzone w formie ćwiczeń wykonywanych w laboratorium (nie dopuszcza się zajęć w formule e-learningu). Środowisko szkoleniowe powinno być dostarczone w modelu mobilnym (mobilne stanowisko pracy) z możliwością uruchomienia na dowolnym komputerze PC wyposażonym w porty USB 2.0/3.0 (np. Windows To Go o pojemności min. 128GB). Czas trwania szkolenia minimum 24 godziny lekcyjne. Szkolenie musi zostać przeprowadzone przez trenera posiadającego certyfikaty MCP/MCSA/MCSE/MCTS oraz musi być przeprowadzone w autoryzowanym ośrodku szkoleniowym zlokalizowanym w tej samej miejscowości co siedziba Zamawiającego.

Zamawiający wymaga, aby szkolenie zostało przeprowadzone w terminie do 180 dni od dnia dostarczenia dokumentu potwierdzającego wykupienie usługi przedłużenia gwarancji, licencji na aktualizację oprogramowania oraz wsparcia technicznego i podpisania protokołu odbioru. Wykonawca, na potwierdzenie rezerwacji szkolenia, zobowiązany jest dostarczyć, w terminie do 7 dni od dnia zawarcia umowy w sprawie zamówienia publicznego, vouchery o terminie ważności szkolenia do 180 dni od dnia dostarczenia dokumentu potwierdzającego wykupienie usługi świadczenia przedłużenia gwarancji, licencji na aktualizację oprogramowania oraz wsparcia technicznego i podpisania protokołu odbioru.