Szczegółowy opis przedmiotu zamówienia – Część I

Przedmiotem zamówienia – dla Części I - jest przedłużenie, na okres wynikający z oferty Wykonawcy (nie krócej jednak niż na 36 miesięcy), serwisu pogwarancyjnego realizowanego przez producenta urządzenia dla użytkowanej przez Zamawiającego macierzy dyskowej Netapp FAS2240. Dotychczasowe wsparcie techniczne wygasa w dniu 30.06.2016 r. Numery seryjne kontrolerów macierzy będących w posiadaniu Zamawiającego:

Macierz	**Numery seryjne kontrolerów**
Netapp FAS2240	210000050313, 600000280824

Zamawiający wymaga świadczenia serwisu pogwarancyjnego producenta na poziomie **SupportEdge Standard,** tj.: serwis pogwarancyjny będzie świadczony przez producenta w trybie całodobowej gotowości przez 7 dni w tygodniu (tryb 24/7), z czasem reakcji na awarie krytyczne do dwóch godzin i wymianą uszkodzonych elementów z asystą inżyniera na następny dzień roboczy po diagnozie problemu. W ramach świadczonego serwisu pogwarancyjnego, Zamawiający otrzyma dostęp do bazy wiedzy producenta, dostęp do najnowszych wersji oprogramowania, dostęp do usługi automatycznego powiadamiania centrum serwisowego producenta o stanie macierzy. Uszkodzone dyski pozostają własnością Zamawiającego.

Zamawiający wymaga, aby zakupiona usługa serwisu pogwarancyjnego producenta pochodziła z autoryzowanego kanału sprzedaży producenta urządzenia na rynek Polski.

Zamawiający wymaga, aby podmiot realizujący zamówienie posiadał status partnerski producenta na poziomie GOLD, tj.: posiadał autoryzację producenta pamięci masowych firmy Netapp oraz dysponował wykwalifikowanymi inżynierami systemowymi posiadającymi certyfikat Netapp Accredited Storage Architect Professionals.

Szkolenie

Integralną częścią zakupu usługi wsparcia technicznego dla macierzy dyskowych będzie przeszkolenie 3 pracowników wskazanych przez Zamawiającego z zakresu podstaw bezpieczeństwa w środowiskach Windows Client (7/8.1/10) oraz Windows Server (2008R2/2012R2/2016). Szkolenie musi obejmować następującą tematykę:

1) zapoznanie z typowymi atakami przeciwko urządzeniom sieciowym, zagrożeniami i podatnościami na ataki oraz poznanie działań wykonywanych przez personel, odpowiedzialny za bezpieczeństwo do zabezpieczenia urządzeń sieciowych;
2) zapoznanie ze sposobami wykorzystania kryptografii do zabezpieczania informacji i nabycia umiejętności wyboru odpowiedniej dla organizacji metody szyfrowania;

3) zabezpieczanie informacji w organizacji przy użyciu uwierzytelniania oraz kontroli dostępu;
4) dystrybucja i zarządzanie certyfikatami;
5) zabezpieczanie transmisji danych poprzez identyfikację zagrożeń dla urządzeń sieciowych oraz implementacja zabezpieczeń dla typowych metod transmisji danych, zdalnego dostępu i sieci bezprzewodowych;
6) zabezpieczanie serwerów WWW przeciwko typowym atakom i konfiguracja zabezpieczenia przeglądarek internetowych;
7) zabezpieczanie wiadomości e-mail i komunikatorów internetowych przed typowymi zagrożeniami;
8) zapoznanie z typowymi zagrożeniami usług katalogowych i DNS oraz zastosowanie metod zabezpieczających te usługi;
9) zapoznanie z zagrożeniami dla peryferiów sieci i monitorowanie ich zabezpieczeń;
10) zapoznanie polis zabezpieczeń służących do zarządzania bezpieczeństwem wykonywanych operacji i wykorzystanie tych polis;
11) zapewnienie nieprzerwanego działania przez implementację bezpiecznej strategii odzyskiwania sprawności po awarii, minimalizacji zagrożeń w komunikacji oraz tworzenia bezpiecznych kopii bezpieczeństwa i ich odtwarzania;
12) identyfikacja, odpowiedź na incydenty oraz asystowanie przy formalnym śledztwie w przypadku włamania.

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 minimum 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 świadczenia serwisu pogwarancyjnego 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 serwisu pogwarancyjnego i podpisania protokołu odbioru.