Załącznik nr 6 do SWZ

Nr postępowania: 11/2024.

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia Modernizacja infrastruktury serwerowej oraz sieciowej w SP ZOZ MSWiA w Szczecinie w oparciu o sprzęt otrzymany w ramach projektu e-Zdrowie.

I Przedmiot zamówienia:

Wykonawca wykona w ramach zadania wdrożenie posiadanego przez zmawiającego sprzętu oraz oprogramowania.

II Miejsce realizacji zamówienia:

1. SP ZOZ MSWiA w Szczecinie, ul. Jagiellońska 44, 70-382 Szczecin,
2. Poradnia POZ oraz Poradnia Zdrowia Psychicznego, ul. Królowej Korony Polskiej 5/6, 70-490 Szczecin,
3. Zakład Rehabilitacji Leczniczej oraz Stomatologia, ul. Piotra Skargi 16, 71-422 Szczecin.

III Podstawa wykonania:

1. Podstawa wykonania zamówienia:
   Zamawiający informuje, iż ze względu na specyfikę przedmiotu zamówienia (w celu prawidłowego przygotowania oferty oraz oszacowania kosztów realizacji zamówienia) złożenie oferty musi być poprzedzone odbyciem wizji lokalnej. Z odbycia wizji lokalnej zostanie sporządzony protokół podpisany przez obie strony, który będzie stanowił potwierdzenie odbycia wizji lokalnej.
   Przed przystąpieniem do wizji lokalnej, uczestnicy będą zobowiązani do podpisania oświadczenia o zachowania tajemnicy i poufności uzyskanych informacji o infrastrukturze, której dotyczy zamówienie.
   Miejsce wizji lokalnej jest tożsame z miejscem realizacji zamówienia.
   Szacowany czas potrzebny na odbycie wizji: 8h.
2. Lista sprzętu objętego wdrożeniem:
   a) serwer rack Dell PowerEdge R750 – 6szt.,
   b) przełącznik Cisco C9500 – 4 szt.,
   c) przełącznik Cisco C9200 – 12szt.,
   d) przełącznik FC Brocade DS-6610B – 4szt.,
   e) przełącznik Aruba 6100 – 1szt.,
   f) przełącznik Aruba 2540 JL357A – 5szt.,
   g) UTM Fortigate 100F – 4szt.,
   h) macierz dyskowa Dell UNITY XT 2szt.,
   i) biblioteka taśmowa PowerVault ML3 – 1szt.
3. Lista oprogramowania objętego wdrożeniem:
   a) Windows Server Datacenter 2022,
   b) Windows Server Standard 2022,
   c) VMware ESS/STD,
   d) Veeam Backup & Replication.

IV Zakres prac w środowisku serwerowym:

1. Wdrożenie serwera wraz z macierzą dyskową w serwerowni zapasowej (środowisko zapasowe) – środowisko oparte o jeden serwer fizyczny (serwer aplikacyjny 3) oraz współdzielony zasób macierzowy.
   1) aktualizacja oprogramowania układowego (firmware) do najnowszej wersji na wszystkich urządzeniach wchodzących w skład środowiska zapasowego;
   2) podłączenie macierzy dyskowej i serwera fizycznego do przełączników rdzeniowych z wykorzystaniem portów 10Gb SFP+ z zachowaniem redundancji połączeń fizycznych obsługujących sieć LAN oraz SAN wraz z zapewnieniem dostępu do modułów konfiguracyjnych urządzeń za pomocą wydzielonej sieci zarządzania;
   3) konfiguracja przełączników FC oraz wyznaczenie stref dla poszczególnych systemów;
   4) konfiguracja serwera, macierzy dyskowej i oprogramowania w taki sposób, aby możliwe było uruchomienie protokołu FC. Wymagana jest pełna konfiguracja HyperVisora oraz systemów

operacyjnych i sprzętu. Zamawiający wymaga takiej konfiguracji, aby zapewnić wielościeżkowość w odniesieniu do serwera i macierzy dyskowej z wykorzystaniem protokołu FC. Zamawiający wymaga, aby system działał w klastrze wysokiej dostępności wraz z serwerami (o tej samej funkcji) znajdującymi się w serwerowni głównej;
5) konfiguracja wirtualizacji opartej o system Vmware Vsphere;
6) instalacja wirtualnych systemów operacyjnych wg. Zamawiającego na potrzeby przeniesienia ról i podniesienia wersji obecnych maszyn wirtualnych ze środowiska produkcyjnego;
7) konfiguracja wirtualnych przełączników z uwzględnieniem 26 podsieci wirtualnych, które już istnieją w infrastrukturze;
8) inne informacje konieczne do skonfigurowania serwera wraz z macierzą dyskową będą wynikać z wizji lokalnej w siedzibie Zamawiającego oraz zostaną przedstawione w protokole.

2. Wdrożenie systemu backup Veeam Backup and Replication w serwerowni zapasowej (środowisko zapasowe) – środowisko oparte o jeden serwer fizyczny (serwer backup) oraz bibliotekę taśmową.
   1) aktualizacja oprogramowania układowego (firmware) do najnowszej wersji na wszystkich urządzeniach wchodzących w skład systemu backupowego;
   2) konfiguracja połączeń z HyperVisorami maszyn wirtualnych, magazynów danych, transporterów;
   3) konfiguracja zadań kopii danych maszyn wirtualnych w taki sposób, aby żadne zadanie nie było wykonywane za pomocą agenta;
   4) konfiguracja biblioteki taśmowej:
      a) podłączenie do przełączników rdzeniowych**,**
      b) integracja z systemem kopii zapasowej Veeam Backup and Replication,
      c) utworzenie zadań kopii zapasowej.
   5) inne informacje konieczne do skonfigurowania systemu backupowego wraz z biblioteką taśmową będą wynikać z wizji lokalnej w siedzibie Zamawiającego oraz zostaną przedstawione w protokole.

3. Modernizacja środowiska produkcyjnego – środowisko oparte o dwa serwery fizyczne (serwer aplikacyjny 1 i serwer aplikacyjny 2) oraz współdzielony zasób macierzowy.
   1) migracja maszyn wirtualnych ze środowiska produkcyjnego na wcześniej przygotowane środowisko zapasowe.
      a) migracja obejmuje konwersję około 40 serwerów wirtualnych, które obecnie wchodzą w skład środowiska produkcyjnego i pełnią one funkcję głównie serwerów aplikacyjnych lub przygotowanie maszyn wirtualnych wg. zaleceń Zamawiającego na potrzeby przeniesienia ról z obecnych serwerów produkcyjnych;
   2) po uprzedniej migracji maszyn wirtualnych ze środowiska produkcyjnego oraz weryfikacji poprawności działania Wykonawca usunie wszelkie dane i systemy na tym środowisku i przystąpi do wykonania prac jak w środowisku zapasowym:
      a) aktualizacja oprogramowania układowego (firmware) do najnowszej wersji na wszystkich urządzeniach wchodzących w skład środowiska produkcyjnego,
      b) podłączenie macierzy dyskowej i serwerów fizycznych do przełączników rdzeniowych z wykorzystaniem portów 10GB SFP+ z zachowaniem redundancji połączeń fizycznych obsługujących sieć LAN i SAN wraz z zapewnieniem dostępu do modułów konfiguracyjnych urządzeń za pomocą wydzielonej sieci zarządzania,
      c) konfiguracja przełączników FC oraz wyznaczenie stref dla poszczególnych systemów,
      d) konfiguracja serwerów, macierzy dyskowej i oprogramowania w taki sposób, aby możliwe było uruchomienie protokołu FC. Wymagana jest pełna konfiguracja HyperVisora oraz systemów operacyjnych i sprzętu. Zamawiający wymaga takiej konfiguracji, aby zapewnić wielościeżkowość w odniesieniu do serwerów i macierzy dyskowej z wykorzystaniem protokołu FC. Zamawiający wymaga, aby system działał w klastrze wysokiej dostępności wraz z serwerem (o tej samej funkcji) znajdującymi się w serwerowni zapasowej,
      e) konfiguracja wirtualizacji opartej o system Vmware Vpshere wraz z Vcenter,
      f) konfiguracja wirtualnych przełączników z uwzględnieniem 26 podsieci wirtualnych, które już istnieją w infrastrukturze;
   3) integracja z systemem kopii zapasowej backup Veeam Backup and Replication;
   4) inne informacje konieczne do skonfigurowania serwera wraz z macierzą dyskową będą wynikać z wizji lokalnej w siedzibie Zamawiającego oraz zostaną przedstawione w protokole.

4. Wdrożenie środowiska bazodanowego – środowisko oparte o dwa serwery fizyczne (serwer bazodanowy 1 i serwer bazodanowy 2) rozmieszczone w serwerowniach głównej oraz zapasowej:
   1) aktualizacja oprogramowania układowego (firmware) do najnowszej wersji na wszystkich urządzeniach wchodzących w skład środowiska bazodanowego;
   2) podłączenie do sieci LAN za pomocą interfejsów 10Gb SFP+ oraz sieci SAN interfejsami 16Gb SFP+;
   3) zapewnienie dostępu do modułów konfiguracyjnych urządzeń za pomocą wydzielonej sieci zarządzania;
   4) serwer bazodanowy 1 będzie przechowywał bazy systemów AMMS/InfoMedica/ Laboratorium natomiast serwer bazodanowy 2 będzie przechowywał bazę systemu Chazon oraz PACS. W przypadku awarii jednej z serwerowni Zamawiający wymaga, aby serwery bazodanowe były skonfigurowane w taki sposób, aby możliwa była replikacja poprzez macierz dyskową lub zgodnie z innymi ustaleniami, które będą wynikać z wizji lokalnej;
   5) inne informacje konieczne do skonfigurowania serwera wraz z macierzą dyskową będą wynikać z wizji lokalnej w siedzibie Zamawiającego oraz zostaną przedstawione w protokole.

   Instalacja systemów operacyjnych oraz migracja baz danych będzie wykonana przez firmy partnerskie sprawiające opiekę serwisową nad systemami medycznymi w zakresie systemów: AMMS/InfoMedica/Laboratorium oraz Chazon/PACS.

5. Wdrożenie systemu replikacji pomiędzy środowiskiem produkcyjnym oraz środowiskiem zapasowym (serwery aplikacyjne):
   1) należy przeprowadzić migrację systemów ze środowiska zapasowego na uprzednio przygotowane środowisko produkcyjne zgodnie z wytycznymi Zamawiającego;
   2) do replikacji należy wykorzystać funkcjonalność oferowaną przez macierz dyskową;
   3) środowisko musi zostać skonfigurowane w taki sposób, aby w momencie awarii środowiska produkcyjnego, administrator miał możliwość przełączenia systemów krytycznych na środowisko zapasowe. Systemy krytyczne będą uprzednio wskazane przez Zamawiającego;
   4) inne informacje konieczne do skonfigurowania serwera wraz z macierzą dyskową będą wynikać z wizji lokalnej w siedzibie Zamawiającego oraz zostaną przedstawione w protokole.

6. Rekonfiguracja usługi katalogowej opartej o Microsoft Active Directory.
   1) audyt obecnego kontrolera domeny pod kątem poprawności działania usługi katalogowej;
   2) przygotowanie schematu usługi katalogowej (struktura, polityki, zasady grup, role administracyjne);
   3) wdrożenie usługi katalogowej opartej na oprogramowaniu Windows Server 2022 Standard w trakcie migracji na nowe środowisko wirtualne Vmware dla dwóch maszyn wirtualnych;
   4) rekonfiguracja serwera usługi katalogowej (domena, replikacja, DNS, backup) oraz wdrożenie nowych polityk;
   5) usunięcie nieprawidłowości wynikających z uprzednio przeprowadzonego audytu.

   Projekt obejmuje wdrożenie spójnych polityk zabezpieczeń mających na celu podniesienie poziomu bezpieczeństwa systemu, oraz centralne sterowanie ustawieniami systemów włączonych do usług katalogowych.

V Zakres prac w środowisku sieciowym:

1. Wdrożenie dwóch dodatkowych urządzeń UTM – Fortinet Fortigate 100F w serwerowni produkcyjnej w celu utworzenia klastra wysokiej dostępności składającego się z 4 urządzeń.
   1) montaż urządzeń w szafie RACK;
   2) aktualizacja oprogramowania układowego (firmware) do najnowszej wersji;
   3) połączenie wszystkich urządzeń w klaster pracujący w trybie Active/Passive;
   4) utworzenie interfejsów sieciowych oraz nadanie adresu IP;
   5) konfiguracja dostępu poprzez SSH, oraz HTTPS;
   6) zmiana hasła dostępu;
   7) utworzenie do 100 reguł bezpieczeństwa;
   8) konfiguracja funkcjonalności VPN, oraz utworzenie tuneli Site to Site;
   9) włączenie funkcjonalności Deep Packet Inspection (DPI);
   10) inne informacje konieczne do skonfigurowania serwera wraz z macierzą dyskową będą wynikać z wizji lokalnej w siedzibie Zamawiającego oraz zostaną przedstawione w protokole.
2. Przystosowanie do nowego środowiska czterech przełączników agregujących CISCO C9500, czterech przełączników SAN FC Brocade oraz czterech przełączników serwerowych CISCO C9200.
   1) audyt obecnych ustawień;

2) aktualizacja oprogramowania układowego (firmware) do najnowszej wersji na wszystkich urządzeniach;
3) połączenie przełączników agregujących w klaster StackWise-V składający się z 4 urządzeń;
4) konfiguracja dostępu poprzez SSH;
5) zmiana haseł dostępu;
6) utworzenie wymaganych podsieci wirtualnych VLAN;
7) konfiguracja funkcjonalności Spanning Tree, którą należy skonfigurować na wszystkich przełącznikach w sieci;
8) konfiguracja funkcjonalności Loop Protect;
9) konfiguracja SNMP w celu monitorowania przełącznika;
10) przepięcie wszystkich przewodów światłowodowych z poprzedniego wykorzystywanego przełącznika Extreme Networks S4;
11) wdrożenie redundantnych połączeń między urządzeniami znajdującymi się w środowisku produkcyjnym a zapasowym;
12) inne informacje konieczne do skonfigurowania serwera wraz z macierzą dyskową będą wynikać z wizji lokalnej w siedzibie Zamawiającego oraz zostaną przedstawione protokole.

3. Przeniesienie funkcjonalności routingu z przełącznika pracującego w warstwie L3 Extreme Networks S4 na nowo utworzony klaster urządzeń UTM Fortigate 100F za pośrednictwem przełączników agregujących.
   1) audyt obecnych ustawień;
   2) wyłączenie funkcjonalności L3 na urządzeniu Extreme S4;
   3) utworzenie nowych interfejsów na urządzeniu Fortigate;
   4) utworzenie polityk bezpieczeństwa;
   5) demontaż urządzenia Extreme S4.
4. Wymiana aktualnie wykorzystywanych przełączników typu ACCESS – Extreme Networks B5 na nowo zakupione przełączniki Cisco C9200, Aruba 6100 oraz Aruba JL677A. Przełączniki należy zainstalować w 10 punktach dystrybucyjnych znajdujących się na terenie szpitala MSWiA:
   1) montaż urządzeń w szafie RACK;
   2) podłączenie w sposób redundantny z przełącznikiem agregującym;
   3) aktualizacja oprogramowania układowego (firmware) do najnowszej wersji na wszystkich urządzeniach;
   4) połączenie urządzeń w stos StackWise wykorzystując dedykowane przewody (jedynie w punktach dystrybucyjnych, gdzie znajduje się powyżej jednego przełącznika);
   5) konfiguracja dostępu poprzez SSH;
   6) zmiana haseł dostępu;
   7) nadanie adresu IP;
   8) konfiguracja podsieci wirtualnych VLAN;
   9) uruchomienie protokołu Loop Protect;
   10) konfiguracja protokołu Spanning Tree;
   11) konfiguracja SNMP w celu monitorowania przełącznika;
   12) przełączenie stacji roboczych podłączonych do przełączników Extreme Networks B5 na nowe przełączniki w punktach dystrybucyjnych;
   13) demontaż nieużywanych urządzeń z szaf RACK;
   14) inne informacje konieczne do skonfigurowania serwera wraz z macierzą dyskową będą wynikać z wizji lokalnej w siedzibie Zamawiającego oraz zostaną przedstawione w protokole.

VI Przeprowadzenie testów penetracyjnych:

Wykonawca przeprowadzi testy podatności systemów (testy penetracyjne). Testy będą polegały na zdalnej enumeracji otwartych portów oraz weryfikacji bezpieczeństwa oprogramowania na nich nasłuchującego. Skanowanie obejmie:

1) urządzenia dedykowane na przykład routery oraz przełączniki;
2) punkty styku z sieciami obcymi;
3) zbadanie podatności systemów Zamawiającego na ataki przeprowadzane z zewnątrz.

Ponadto Wykonawca przeprowadzi badanie bezpieczeństwa sieci systemów komputerowych, które pozwoli m.in. na określenie błędów w konfiguracji skutkujących powstaniem podatności na atak oraz wskazanie nadmiernych uprawnień, niezgodnych z zasadami dobrych praktyk. Badaniu będą podlegały systemy z rodziny Microsoft Windows Server, Linux oraz CISCO.

Realizacja testów podatności systemów będzie zakończona raportem, którego forma oraz zakres będą zawarte w protokole sporządzonym po odbyciu przez Wykonawcę wizji lokalnej.

VII Informacje ogólne:

1. Wykonawca winien wykonać wszelkie prace zabezpieczające mające na celu niedopuszczenie do uszkodzeń urządzeń, których właścicielem jest Zakład SP ZOZ MSWiA w Szczecinie.
2. Wykonawca winien przygotować dokumentację powykonawczą.
3. Wykonawca jest zobowiązany do organizowania prac w sposób zapewniający ciągłość działania Zakładu SP ZOZ MSWiA w Szczecinie.

Wszystkie prace związane z zakresem prac w środowisku serwerowym oraz sieciowym wykonywane będą w siedzibie Zamawiającego