Zał. nr 1b do Og.271.ZO.4.2023

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiot zamówienia został podzielony na dwie części:

Część I - Modernizacja infrastruktury sieciowej oraz zapewnienie systemu monitoringu stanu infrastruktury IT Zamawiającego

Część II - Szkolenie z zakresu cyberbezpieczeństwa

OPIS PRZEDMIOTU ZAMÓWIENIA CZĘŚCI I

Modernizacja infrastruktury sieciowej

1. Przedmiotem zamówienia jest:

1) utworzenie nowej infrastruktury sieciowej LAN w siedzibie Zamawiającego składającej się z 66 nowych punktów dostępowych sieci LAN rozlokowanych w obrębie budynku wraz z niezbędnymi akcesoriami:
   a. patchpanel kat. 6, 24-portowy – 3 sztuki
   b. organizer kabli do szafy RACK – 3 sztuki
2) dostawa fabrycznie nowego Sprzętu, nie używanego w innych środowiskach ani projektach, w ilościach:
   a. Przełącznik sieciowy – 2 sztuki
   b. Punkt dostępowy - 4 sztuki
   c. Wkładki SFP+ kompatybilne z przełącznikami sieciowymi z pkt a. - 4 sztuki
   d. Dostarczenie patchcordów światłowodowych kompatybilnych z wkładkami z pkt c. - 2 sztuki
3) konfiguracja urządzeń oraz fizyczna instalacja w infrastrukturze IT Zamawiającego;
4) udzielenie przez Wykonawcę gwarancji i zapewnienie w jej ramach serwisu gwarancyjnego oraz wsparcia technicznego na dostarczony Sprzęt;
5) dostarczenie przez Wykonawcę dokumentacji dostarczonego Sprzętu;

2. Wymagania odnośnie prac instalatorskich

1) Demontaż istniejących koryt kablowych w infrastrukturze Zamawiającego z jednoczesnym zachowaniem funkcjonalności istniejącej sieci
2) Wykonanie nowych przewiertów pomiędzy piętrami, niezbędnych przewiertów w ciągu korytarzy wynikających z ich ukształtowania oraz z korytarzy do poszczególnych pokoi
3) Uzgodnienie z Zamawiającym miejsca montażu lokalizacji poszczególnych punktów dostępowych sieci LAN.
4) Wykonawca zobowiązuje się do wykonania montażu nowych, dostarczonych przez z siebie koryt kablowych w obrębie korytarzy oraz w pomieszczeniach
5) Wykonawca zobowiązuje się dostarczyć wymagane okablowanie minimum w kategorii 6 - skrętka UTP i umieścić je w zainstalowanych korytach

6) Wykonawca zobowiązuje się poprowadzić nowe okablowanie od punktów dystrybucyjnych do punktów logicznych oraz dokonać obróbki, montażu i rozszycia kabli w panelach w szafach dystrybucyjnych
7) Zamawiający wymaga, aby na zakończenie prac Wykonawca zamknął wszystkie zamontowane koryta kablowe z umieszczoną w nich nową instalacją teleinformatyczną, wykonał testy poprawności działania oraz opisy gniazd po stronie punktu dystrybucyjnego oraz na gniazdach dostępowych
8) Po wykonaniu testów i opisów Wykonawca jest zobowiązany do przełączenia użytkowników do nowej infrastruktury
9) Po wykonaniu przełączenia użytkowników Wykonawca jest zobowiązany do usunięcia starego okablowania oraz wykonania drobnych prac naprawczo malarskich

3. Zestawienie wymaganych parametrów technicznych dla przełączka sieciowego (2 sztuki)

Interfejs sieciowy	48x 1Gb Ethernet (10/100/1000 Mbps) 4x SFP+ (1/10 Gbps)
Interfejs zarządzania	Ethernet, In-Band
Łączna przepustowość (non-blocking)	Minimum 88 Gbps
Przepustowość przełączania	Minimum 176 Gbps
Prędkość przekazywania	Minimum 130 Mpps
Sposób zasilania	Uniwersalny: 100 - 240 V AC / 50 - 60 Hz USP RPS DC: 52VDC, 11.54A; 11.5VDC, 5.22A
Zasilacz	Wbudowany, AC/DC Moc minimum 650 W
Maksymalny pobór mocy	Bez zasilania PoE: maksymalnie 60 W
Diody LED	System: Status RJ45: PoE; Speed / Link / Activity SFP+: Link / Activity
Waga	Z uchwytami montażowymi: maksymalnie 6,40 kg Bez uchwytów montażowych: maksymalnie 6,30 kg
Dopuszczalna temperatura pracy	Od -5 do 40 st. C
Certyfikaty	IC, FCC, CE
Możliwość montażu w szafie RACK	Tak, maksymalnie 1U
PoE	
Interfejsy	40 x PoE+ IEEE 802.3af/at 8 x 60W PoE++ IEEE 802.3af/at/bt
Maksymalny budżet PoE	600 W

Maksymalna moc PoE	Dla 802.3at: minimum 30 W Dla 802.3bt: minimum 62W
Zakres napięcia	Dla 802.3af: 44-57 V Dla 802.3at/bt: 50-57 V

4. Zestawienie wymaganych parametrów technicznych dla punktu dostępowego (4 sztuki)

Interfejs sieciowy	2 x 1 Gbit/s RJ-45
Maksymalna przepustowość w paśmie 2,4 GHz	450 Mbit/s
Maksymalna przepustowość w paśmie 5 GHz	1300 Mbit/s
MIMO dla pasma 2,4 GHz	3x3
MIMO dla pasma 5 GHz	3x3
Obsługa PoE	802.3af PoE oraz 802.3at PoE+
Montaż	Ściana/sufit
Maksymalny pobór mocy	9W
Dodatkowe interfejsy	1x USB
Obsługiwane standardy WIFI	802.11 a/b/g/n/r/k/v/ac
Obsługiwane protokoły zabezpieczeń	WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)
VLAN	Zgodnie ze standardem 802.1Q
Obsługiwana liczba użytkowników jednocześnie	Minimum 124
Temperatura pracy	-10 do 70 °C
Maksymalne wymiary	196,7 x 196,7 x 35 mm
Certyfikacja	CE, FCC, IC

5. Zestawienie wymaganych parametrów technicznych wkładek SFP+ (4 sztuki)

Interfejs sieciowy	10 Gbit/s SFP+ LC
Maksymalny pobór mocy	1W
Maksymalny dystans	10 km
Temperatura pracy	0 do 70 °C

6. Zestawienie wymaganych parametrów technicznych dla patchcordów światłowodowych

Interfejs sieciowy	LC

Maksymalna długość	1m

7. Wymagania ogólne dla przełączników sieciowych, punktów dostępowych oraz wykonywanych prac:

1) Dostarczone urządzenia muszą być objęte gwarancją opartą o świadczenia gwarancyjne producenta sprzętu, niezależnie od statusu partnerskiego Wykonawcy przez okres co najmniej 12 miesięcy
2) Urządzenie musi mieć możliwość zarządzania i konfigurowania poprzez dedykowane rozwiązanie zarządzające, posiadające funkcje takie jak:
    a. podgląd statusu urządzeń w czasie rzeczywistym
    b. centralne zarządzanie wieloma sieciami z poziomu interfejsu graficznego
    c. możliwość zdalnej aktualizacji oprogramowania urządzeń
    d. wersję mobilną aplikacji
3) Przełączniki muszą być zarządzalne w warstwie 2 i 3
4) Zaproponowane rozwiązania odnośnie przełączników sieciowych oraz punktów dostępowych, muszą być kompatybilne i wyprodukowane przesz tego samego producenta
5) Dostarczający jest zobowiązany do podłączenia urządzeń sieciowych w infrastrukturze Zamawiającego do wskazanych miejsc połączeń sieciowych i elektrycznych
6) Dostarczający jest zobowiązany do aktualizacji oprogramowania sprzętowego dostarczonych urządzeń do najnowsze dostępnej i zalecanej przez producenta wersji
7) Dostarczający musi utworzyć dostępy administracyjne do urządzeń oraz przekazać je Zamawiającemu
8) W ramach przekazanych urządzeń, Wykonawca zobowiązuje się - na wskazanych przez Zamawiającego interfejsach - zdefiniować do 4 VLAN-ów
9) Na wskazanym przez Zamawiającego zasobie serwerowym, Wykonawca zobowiązany jest do instalacji, konfiguracji i dodania urządzeń sieciowych do dedykowanego centralnego rozwiązania zarządzającego

<u>Zapewnienie systemu monitoringu stanu infrastruktury IT Zamawiającego:</u>

1) dostawa systemu monitoringu dla infrastruktury IT Zamawiającego;
2) przeprowadzenie szkolenia z posługiwania się dostarczonym rozwiązaniem i interpretacji danych prezentowanych przez system monitoringu.

1. Szczegółowe wymagania odnośnie proponowanego rozwiązania

1) System powinien być uruchomiony na zasobach infrastruktury IT Zamawiającego.
2) System powinien być zrealizowany na środowisku nie wymagającym licencjonowania systemu operacyjnego maszyny wirtualnej
3) System powinien agregować dane o statusie maszyn wirtualnych realizowanych na wirtualizatorze Microsoft HYPER-V oraz VMWare
4) W przypadku systemów z rodziny Microsoft Windows Server oraz Linux, system powinien zapewniać możliwość zdefiniowania kluczowych usług, których wyłączenie lub przerwa w działaniu będzie monitowana - serwisów uruchomionych na powłoce Windows/Linux, statusu baz danych MSSQL Express i Standard, PostgresSQL, Firebird
5) System musi zapewniać możliwość odczytu danych z urządzeń przy wykorzystaniu protokołu SNMP, IMPI, JMX

6) System musi zapewniać możliwość ostrzegania w przypadku braku odpowiedzi z monitorowanego urządzenia, maszyny wirtualnej, serwera fizycznego
7) W przypadku rozwiązań serwerowych system musi zapewniać możliwość odczytu danych o statusie temperatury procesora, płyty głównej dla wiodących vendorów takich jak Lenovo, HP, DELL
8) System powinien integrować się z rozwiązaniami do zdalnego zarządzania serwerami takimi jak: iDRAC, iLO, XClarity Controller
9) System powinien pozwalać. na uzyskiwanie informacji o utylizacji CPU, RAM, przestrzeni pamięci masowej, interfejsów sieciowych maszyn wirtualnych opartych o Linux, Windows
10) System powinien zapewniać możliwość odczytu stanu CPU, wentylatorów, temperatury, utylizacji interfejsów urządzeń sieciowych wiodących producentów jak Ubiquiti, DELL, Extreme, Fortinet, CISCO i innych zapewniających komunikację SNMP z urządzeniem
11) System powinien umożliwiać dla monitorowanych elementów natychmiastowe graficzne przedstawienie na wykresie za pomocą wbudowanej funkcjonalności
12) System graficznego przedstawienia (wykresy) powinien posiadać funkcje:
    a. możliwości tworzenia niestandardowych wykresów;
    b. łączenia wielu elementów w jeden widok
    c. tworzenia mapy sieci
    d. tworzenia raportów
13) System powinien mieć funkcjonalność pozwalającą na tworzenie szablonów konfiguracji serwerów
14) System powinien zapewniać możliwość wykonania automatycznego wyrywania urządzeń sieciowych w danym obszarze
15) System powinien zapewniać możliwość automatycznej rejestracji agenta
16) System powinien zapewniać programowalny interfejs API
17) System musi zapewniać możliwość definiowania czasu retencji przechowywania danych oraz progów ostrzeżeń:
    a. Warning – rozumianych jako ostrzeżenie
    b. Critical – rozumianych jako rzutujących na całą infrastrukturę Zamawiającego i uniemożliwiające wykonywanie czynność)
18) System powinien zapewniać możliwość wysyłki monitów w postaci e-mail oraz opcjonalnie powinien zapewniać możliwość integracji z rozwiązaniami typu bramka sms
19) System powinien zapewniać możliwość bezpiecznego uwierzytelniania oraz nadawania wielopoziomowych uprawnień
20) System powinien zapewniać możliwość monitorowania minimum 100.000 obiektów w ramach jednej instancji

2. Wymagane prace wdrożeniowe

1) instalacja przez Wykonawcę rozwiązania na dedykowanym zasobie wirtualnym Zamawiającego;
2) konfiguracja wstępna i nadanie dostępów do logowania dla Zamawiającego;
3) przygotowanie po konsultacji z Zamawiającym monitoringu dla 10 urządzeń wytypowanych przez Zamawiającego (serwery, przełączniki, urządzenie brzegowe klasy UTM);
4) konfiguracja progów alarmów zgodnie z wymogami Zamawiającego oraz po konsultacji z Wykonawcą i wdrożeniem w oparciu o najlepsze praktyki;
5) konfiguracja powiadomień na wskazaną przez Zmawiającego skrzynkę pocztową za pośrednictwem dedykowanej skrzynce technicznej dostarczonej przez Zamawiającego.

Wykonawca udzieli Zamawiającemu gwarancji na dostarczony Sprzęt i urządzenia na okres 24 miesięcy od daty podpisania protokołu odbioru.
Pozostałe warunki gwarancji i rękojmi zostały zawarte w wzorze umowy i karcie gwarancji, który stanowi załącznik nr 2 do Warunków zamówienia.

OPIS PRZEDMIOTU ZAMÓWIENIA CZĘŚCI NR 2

Przedmiotem zamówienia jest przeprowadzenie szkolenia zwiększającego świadomość pracowników Zamawiającego w dziedzinie cyberbezpieczeństwa;

1. Przedmiot zamówienia

1. Odbiorcą szkolenia będą pracownicy Urzędu Gminy w Rogowo podzieleni na dwie grupy.
2. Ilość osób uczestniczących w szkoleniu: około 30 osób.
3. Szkolenie odbędzie się w siedzibie Zamawiającego tj. Urząd Gminy w Rogowie, Rogowo 51, 87-515 Rogowo na Sali konferencyjnej.
4. Szkolenia będą prowadzone dla dwóch grup w godzinach:
   - pierwsza grupa – szkolenie w godzinach od 7:30 do 11:00,
   - druga grupa – szkolenie w godzinach od 11:30 do 15:00.
5. Szkolenie ma odbyć się w jeden dzień roboczy, wcześniej zatwierdzony przez Zamawiającego.
6. Szkolenia będą prowadzone w języku polskim.
7. Szkolenia prowadzone będą na podstawie zaakceptowanego prze Zamawiającego szczegółowego zakresu merytorycznego szkolenia dostarczonego przez Wykonawcę.
8. W trakcie szkolenia przewiduje się jedną przerwę trwającą 15 minut.
9. W ramach organizacji szkoleń Wykonawca zapewni:
   1) Materiały szkoleniowe, obejmujące szczegółowy zakres szkolenia, harmonogram dzienny szkolenia oraz materiały merytoryczne (np. skrypty, podręczniki, zeszyty informacyjne, broszury) w formie papierowej, zawierające szczegółowe informacje, które będą omawiane podczas szkolenia. Ponadto, uczestnicy otrzymają materiały pisarskie, w tym notatniki i długopisy. Materiały szkoleniowe przekazywane są nieodpłatnie Uczestnikom na własność. 2 egzemplarze materiałów szkoleniowych zostaną przekazane Zamawiającemu w celach archiwalnych.
   2) Warunki pracy uczestników i Wykonawcy w trakcie trwania szkolenia zgodne przepisami bezpieczeństwa i higieny pracy.
   3) Wystarczającą liczbę własnych licencji na oprogramowanie komputerowe wykorzystywane przy realizacji szkoleń oraz sprzęt komputerowy dla każdego Uczestnika umożliwiający przeprowadzenie szkolenia.
   4) Właściwe działania promocyjne i informacyjne dotyczące szkoleń, w tym właściwe oznakowanie materiałów szkoleniowych przekazanych Uczestnikom oraz Zamawiającemu w celach archiwalnych z obowiązkowymi oznaczeniami Beneficjentów Funduszy Europejskich.
   5) Wydanie Uczestnikom szkolenia zaświadczeń o ukończeniu danego szkolenia w wersji papierowej.
   6) Kadrę trenerską posiadającą wiedzę i umiejętności adekwatne do rodzaju i zakresu merytorycznego szkolenia, zdolną do pełnej realizacji wymogów związanych z prowadzeniem szkoleń.

7) Prowadzenie dokumentacji szkolenia w właściwy sposób. Na dokumentację szkolenia składają się:
   a) Lista obecności Uczestników szkolenia,
   b) Lista odbioru zaświadczeń o ukończeniu szkolenia.
   c) Potwierdzenie przez Uczestników odbioru materiałów szkoleniowych.
   d) Przeprowadzenie ankiet satysfakcji po szkoleniu.
   e) Sporządzony przez kadrę trenerską dziennik zajęć, zawierający szczegółowe informacje na temat przebiegu oraz zakresu merytorycznego szkolenia, podpisany po zakończeniu szkolenia przez prowadzącego szkolenie.

Przykładowy zakres szkolenia:

1. Główne założenia i wymagania prawne cyberbezpieczeństwa w pracy urzędnika.
2. Polityka bezpieczeństwa w organizacji.
3. Definicja incydentu bezpieczeństwa i zasady postępowania z incydentem.
4. Rodzaje ataków: ataki socjotechniczne, ataki komputerowe, ataki przez sieci bezprzewodowe, ataki przez pocztę e-mail (fałszywe e-maile), ataki przez strony WWW, ataki przez telefon, phishing, spoofing, spam.
5. Bezpieczeństwo fizyczne - urządzenia, dokumenty, „czyste biurko”.
6. Zabezpieczenie informatycznych nośników danych – pendrivy i pamięci zewnętrzne.
7. Zdalny dostęp do zasobów jednostki i korzystanie z urządzeń prywatnych przez pracowników oraz związane z tym potencjalne zagrożenia.
8. Przechowywanie danych w chmurze i korzystanie z zewnętrznych dostawców usług informatycznych.
9. Prawidłowe korzystanie z oprogramowania antywirusowego.
10. Zasady aktualizacji programów i aplikacji.
11. Szyfrowanie dokumentów i poczty elektronicznej.
12. Polityka haseł, zarządzanie dostępem i tożsamością.