

## OPIS PRZEDMIOTU ZAMÓWIENIA

**ZNAK: ZP.271.17.2022**

### **1. Diagnoza cyberbezpieczeństwa**

Usługa polegająca na przeprowadzeniu technicznej diagnozy cyberbezpieczeństwa urzędu z zgodnie z zakresem zawartym w formularzu stanowiącym załącznik nr 8 do Regulaminu Konkursu Grantowego „Cyfrowa Gmina”.

Przedmiot zamówienia będzie realizowały przez osoby posiadające wymagane uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia diagnozy w rozumieniu art. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Wykonawca dostarczy wyniki diagnozy cyberbezpieczeństwa w postaci elektronicznej (opatrzonym podpisem elektronicznym), wypełnionego „Formularza informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa”. Dostarczony plik winien być podpisany przez osobę wykonującą diagnozę, posiadającą uprawnienia wymagane w regulaminie konkursu.

### **2. Wdrożenie systemu do monitorowania środowiska IT.**

Przedmiotem zamówienia jest wdrożenie systemu monitorowania Zabbix (zabbix.com) oraz serwera zbierającego logi z kluczowych urządzeń systemu.

1. Instalacja serwera zabbix jako maszyny wirtualnej uruchamianej na MS Hyper-V.
2. Instalację i konfigurację agentów do monitorowania
  - serwerów fizycznych w ilości 3 szt,
  - maszyn wirtualnych w ilości 5 szt. dla systemów Windows Server i Debian Linux,
  - macierzy dyskowej z systemem FreeNas,
  - przełączników w sieci lan,
  - UMT Stormshield,
  - zasilaczy awaryjnych.
3. Monitorowane mają być
  - podstawowe parametry systemów (obciążenie procesora, zajętość pamięci, ilość wolnego miejsca na dyskach, obciążenie kart sieciowych, itp.),
  - status macierzy dyskowych,
  - dostępność i obciążenie łącza internetowego,
  - temperatura podzespołów serwerów,
  - pobór mocy serwerów,
  - dostępność i wydajność urządzeń sieciowych,
  - statusy portów sieciowych,
  - wskazane usługi.
4. Przeszkolenie 1 osoby z obsługi systemu.
5. Wsparcie powdrożeniowe przez okres 1 roku.

### **3. Rozbudowa zabezpieczeń logicznych**

Przedmiotem zamówienia jest

1. Konfiguracja VLAN osobno dla serwerów, stacji roboczych jednostek (Urząd Gminy, ZEAS, ZGKIM), urzędzeń skanujących i drukujących, telewizji przemysłowej, wi-fi gości, kiosku informacyjnego, zarządzania urządzeniami sieciowymi, serwera z macierzą na kopie zapasowe.
2. Dostarczenie Premium UTM Security Pack (UTM Security Pack + Zaawansowany Antywirus + Audyt Podatności + Rozszerzony filtr URL) do Stormshield SN310 na okres 1 rok
3. Konfiguracja urządzenia Stormshield SN310
  - konfiguracja interfejsów fizycznych i VLAN zgodnie z topologia sieci
  - konfiguracja przełączania pomiędzy dwoma dostawcami Internetu
  - konfiguracja PROXY HTTP, PROXY SMTP, PROXY POP3, PROXY FTP
  - konfiguracja filtra URL
  - konfiguracja połączeń SITE-TO-SITE IPSEC VPN pomiędzy jednostkami (UG, OPS)
  - testowanie wdrożonej konfiguracji
  - strojenie IPS / HTTPS PROXY
- 4. Oprogramowanie do archiwizacji danych.**

Przedmiotem zamówienia jest dostarczenie oprogramowania Xopero One w odpowiedniej ilości licencji oraz jego wdrożenie.

1. Instalacja serwera i konsoli Xopero One jako maszyny wirtualnej uruchamianej na MS Hyper-V.
2. Instalację agentów na 30 komputerach w sieci i 5 serwerach.
3. Konfigurację harmonogramów wykonywania kopii zapasowych – obrazy systemów Windows i Linux, archiwizacja baz MS SQL, archiwizacja plików.

#### **5. Modernizacja sieci komputerowej**

Przedmiotem zamówienia jest dostarczenie sprzętu sieciowego oraz modernizacja okablowania.

1. Dostarczenie
  - 2 szt. przełącznik sieciowy 52 port
  - 1 szt. 28 port
  - 2 szt. transceiver SFP+ 10GBASE współpracujący z dostarczonymi przełącznikami
2. Przeprowadzenie światłowodu pomiędzy budynkami.
3. Porządkowanie okablowania w serwerowni polegające na montażu 2 paneli krosowych i podłączeniu do nich istniejących kabli.

#### **Parametry przełączników**

Klasa przełącznika	SMART
--------------------	-------

Zastosowanie	Średnie i duże firmy
Warstwa przełączania	<ul style="list-style-type: none"> <li>• L2</li> <li>• L2+</li> <li>• L3</li> </ul>
Liczba portów 10/100/1000 Mbps	52 (28)
Liczba portów 10G SFP+	2
Liczba portów 10G Base-T	2
Tryb przekazywania	Store-and-forward
Rozmiar tablicy adresów MAC	8000
Obsługa ramek Jumbo	Nie
Rozmiar ramki Jumbo	10 KB
Możliwość łączenia w stos	Nie
VLAN	<ul style="list-style-type: none"> <li>• Max. 4K VLAN groups</li> <li>• Max. 1~4094 VIDs</li> <li>• GVRP</li> <li>• Max. 4K dynamic VLAN groups</li> <li>• Double VLAN (Q-in-Q)</li> <li>• Port-based Q-in-Q</li> <li>• Selective Q-in-Q</li> <li>• 802.1Q</li> <li>• Auto Surveillance VLAN</li> <li>• Port-based VLAN</li> <li>• 802.1v Protocol-based VLAN</li> <li>• Voice VLAN</li> <li>• MAC-based VLAN</li> <li>• Subnet-based VLAN</li> <li>• VLAN translation</li> <li>• Multicast VLAN (ISM VLAN for IPv4/IPv6)</li> <li>• Asymmetric VLAN</li> <li>• Private VLAN</li> <li>• VLAN Trunking</li> <li>• Super VLAN</li> </ul>
Obsługiwane protokoły i standardy	<ul style="list-style-type: none"> <li>• IEEE 802.3 10BASE-T Ethernet (twisted-pair copper)</li> <li>• IEEE 802.3u 100BASE-TX Fast Ethernet (twisted-pair copper)</li> <li>• IEEE 802.3u 100BASE-FX 100 Mbps over fiber optic</li> <li>• IEEE 802.3ab 1000BASE-T Gigabit Ethernet (twisted-pair copper)</li> <li>• IEEE 802.3z 1000BASE-X 1 Gbps over fiber optic</li> </ul>

	<ul style="list-style-type: none"> <li>• IEEE 802.3az Energy-Efficient Ethernet (EEE)</li> <li>• IEEE 802.3x Flow Control</li> <li>• IEEE 802.3ae 10 Gigabit Ethernet</li> <li>• IEEE 802.3af/at</li> </ul>
QoS	<ul style="list-style-type: none"> <li>• IEEE 802.3 10BASE-T Ethernet (twisted-pair copper)</li> <li>• IEEE 802.3u 100BASE-TX Fast Ethernet (twisted-pair copper)</li> <li>• IEEE 802.3u 100BASE-FX 100 Mbps over fiber optic</li> <li>• IEEE 802.3ab 1000BASE-T Gigabit Ethernet (twisted-pair copper)</li> <li>• IEEE 802.3z 1000BASE-X 1 Gbps over fiber optic</li> <li>• IEEE 802.3az Energy-Efficient Ethernet (EEE)</li> <li>• IEEE 802.3x Flow Control</li> <li>• IEEE 802.3ae 10 Gigabit Ethernet</li> <li>• IEEE 802.3af/at</li> </ul>
Bezpieczeństwo	<p><b>Bezpieczeństwo portu</b></p> <ul style="list-style-type: none"> <li>• Obsługuje do 64 adresów MAC na port</li> <li>• Kontrola burzy Broadcast / Multicast / Unicast</li> <li>• Silnik D-Link Safeguard</li> <li>• Kontrola serwera DHCP</li> <li>• Ochrona źródła IP</li> <li>• DHCP Snooping</li> <li>• Snooping IPv6</li> <li>• Dynamiczna inspekcja ARP (DAI)</li> <li>• Ochrona DHCPv6</li> <li>• Ochrona reklam tras IPv6 (RA)</li> <li>• Inspekcja IPv6 ND</li> <li>• Wykrywanie zduplikowanych adresów (DAD)</li> </ul> <p><b>ARP Spoofing Prevention</b></p> <ul style="list-style-type: none"> <li>• Max. 64 wpisy</li> <li>• Filtrowanie pakietów kontrolnych L3</li> <li>• Przekazywanie odwrotnej ścieżki emisji pojedynczej (URPF)</li> <li>• Segmentacja ruchu</li> </ul> <p><b>SSL</b></p> <ul style="list-style-type: none"> <li>• Obsługuje TLS 1.0 / 1.1 / 1.2</li> <li>• Obsługuje dostęp IPv4 / IPv6</li> </ul>

	<p><b>SSH</b></p> <ul style="list-style-type: none"> <li>• Obsługuje SSH v2</li> <li>• Obsługuje dostęp IPv4 / IPv6</li> <li>• Ochrona przed atakami BPDU</li> <li>• Zapobieganie atakom w systemie DOS</li> </ul>
<p>Zarządzanie, monitorowanie, konfiguracja</p>	<ul style="list-style-type: none"> <li>• Web-based GUI (supports IPv4/IPv6)</li> <li>• Client-based D-Link Network Assistant (DNA)</li> </ul>
<p>Funkcje L2</p>	<ul style="list-style-type: none"> <li>• IGMP v1 / v2 / v3 Snooping</li> <li>• Obsługuje 512 grup IGMP</li> <li>• Oparty na gości IGMP Snooping Fast Leave</li> <li>• Obsługuje 128 statycznych grup IGMP</li> <li>• Per VLAN IGMP Snooping</li> <li>• Uczenie się oparte na danych</li> <li>• IGMP Snooping Querier</li> <li>• Eliminacja raportów</li> <li>• MLD v1 / v2 Snooping</li> <li>• Obsługa 256 grup MLD</li> <li>• Oparty na gości MLD Snooping Fast Leave</li> <li>• Obsługuje 64 statyczne grupy MLD</li> <li>• MLD Snooping Querier</li> <li>• Per VLAN MLD Snooping</li> <li>• Raportowanie proxy MLD</li> </ul>
<p>Funkcje L3</p>	<ul style="list-style-type: none"> <li>• Supports 1024 hardware routing entries shared by IPv4/IPv6</li> <li>• 1 entry consumed by each IPv4 route</li> <li>• 2 entries consumed by each IPv6 route</li> <li>• Supports up to 4096 hardware L3 forwarding entries shared by IPv4/IPv6</li> <li>• 1 entry consumed by each IPv4 route</li> <li>• 2 entries consumed by each IPv6 route</li> <li>• IPv4/IPv6 Static Route</li> <li>• Max. 512 IPv4 entries</li> <li>• Max. 256 IPv6 entries</li> <li>• Equal-Cost Multi-Path Route (ECMP)</li> <li>• Weighted-Cost Multi-Path Route (WCMP)</li> <li>• IPv4/IPv6 Default Route</li> <li>• Policy-based Route (PBR)</li> <li>• Null Route</li> <li>• Route Preference</li> <li>• Route Redistribution</li> <li>• RIPv1/v2/ng</li> <li>• OSPF</li> </ul>

	<ul style="list-style-type: none"><li>• OSPF v2/v3</li><li>• OSPF passive interface</li><li>• Stub/NSSA area</li><li>• Supports Equal-Cost Multi-Path Route (ECMP)</li><li>• Text/MD5 authentication</li></ul>
Typ obudowy	Rack
Wentylator	Tak
Zasilacz	Wewnętrzny

## **6. Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania**

### **7. Edukacja cyfrowa urzędników**

W ramach tego obszaru, zaplanowano szkolenia dla pracowników urzędu w zakresie obsługi zakupionego sprzętu i oprogramowania.

### **8. Szkolenia dla urzędników w zakresie cyberbezpieczeństwa**

Przeprowadzenie szkoleń pracowników z bezpieczeństwa informacji i cyberzagrożeń w kontekście ustawy o KSC oraz Rozporządzenia KRI.

Zagadnienia, które powinny być omówione na szkoleniu:

- Podstawowe przedstawienie zagadnienia cyberbezpieczeństwa;
- Sposoby ochrony kont i danych przed potencjalnym zagrożeniem;
- Ochrona plików i dysków czyli podstawy szyfrowania;
- Logowanie w sieci;
- Częsta zmiana haseł, czy ustalanie ich odpowiedniej trudności,
- Przedstawienie zagrożeń, które czyhają na nas w sieci (rodzaje zagrożeń i ich konsekwencje);
- Utrzymanie bezpieczeństwa informacji w systemach informatycznych (zabezpieczanie środowiska pracy);
- Rozpoznawanie zagrożeń oraz reagowanie na pojawiające się niebezpieczeństwa.

W ramach realizacji szkolenia wymagane jest, aby Szczegółowy harmonogram szkolenia został uzgodniony z Zamawiającym w terminie minimum 14 dni przed terminem rozpoczęcia szkolenia.