Załącznik nr 2– Opis przedmiotu zamówienia

NR SPRAWY: IPR.ZP.271.1.34.2022

ZAMAWIAJĄCY:
Gmina Szreńsk; ul. Plac Kanoniczny 10; 06-550 Szreńsk REGON 130378462, NIP 5691820486
telefon : +(48) 236534038 faks : +(48) 236534038 w. 22
e-mail : szrensk@szrensk.com.pl, www.szrensk.com.pl

OPIS PRZEDMIOTU ZAMÓWIENIA

Poniżej zaprezentowane parametry określają minimalne wymagania Zamawiającego odnośnie wykonanych w ramach Zamówienia przez Wykonawcę usług.

Sporządzenie audytu cyberbezpieczeństwa

Przeprowadzenie audytu cyberbezpieczeństwa w ramach projektu „Cyfrowa Gmina" w Urzędzie Gminy w Szreńsku (w dokumentacji projektu określanego jako „diagnoza cyberbezpieczeństwa") w zakresie oceny zgodności funkcjonujących zasad i procedur dotyczących zarządzania bezpieczeństwem informacji z obowiązującymi aktami prawnymi, w tym, w szczególności weryfikacji struktury organizacji oraz przepływu dokumentów elektronicznych, analizy zewnętrznej i wewnętrznej sieci komputerowej, analizy serwerów, testów dostępu do sieci wewnętrznej i zewnętrznej, analizy stacji roboczych, analizy kopii zapasowych, analizy poczty elektronicznej, analizy ogólnego bezpieczeństwa danych i mechanizmów kontroli w Urzędzie, wraz z przygotowaniem raportu z audytu.

Audyt musi zostać przeprowadzony zgodnie z Ustawą z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369 z późn. zm.) oraz Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247 z pózn. zm.).

Szczegółowy zakres przedmiotu zamówienia zawiera formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa stanowiący załącznik nr 8 konkursu grantowego załączony do niniejszego Zapytania ofertowego jako Załącznik nr 3.

Wykonawca zobowiązany jest do przedstawienia wyników audytu w formie papierowej oraz elektronicznej.

Rozbudowa zabezpieczeń logicznych (firewall, systemy IDS, IPS)

W ramach usługi Urząd zostanie doposażony w zabezpieczenia logiczne (firewall, systemy IDS, IPS). Będą to systemy ochrony do wykrywania i zapobiegania włamaniom. To urządzenia sieciowe zwiększające bezpieczeństwo sieci komputerowych przez wykrywanie (IDS) lub wykrywanie i blokowanie ataków (IPS) w czasie rzeczywistym. IDS służy do monitorowania zagrożeń i incydentów naruszenia bezpieczeństwa oraz do powiadamiania o nich. Z kolei IPS podejmuje dodatkowo działania mające na celu powstrzymanie ataku, minimalizację jego skutków lub aktywną odpowiedź na naruszenie bezpieczeństwa. Tak więc, rozwiązania te umożliwią zwiększenie poziomu bezpieczeństwa sieci komputerowej poprzez wzmocnienie kontroli komunikacji pomiędzy sieciami o różnym stopniu zaufania.

Parametry techniczne

Urządzenie zabezpieczające Firewall/UTM zabezpieczające min 30 stacji roboczych oraz serwerów – 1 szt.	FW+IPS, VPN, filtr URL, AV, AS, DLP, Obsługa kart SD Parametry urządzenia i specyfikacja sieciowa 8 portów Ethernet 10/100/1000 Mbps przepustowość firewalla z włączonym IPS (Gbps) min. 2,400 przepustowość IPSec VPN (Mbps) min. 600 liczba równoległych sesji min. 300 000 nielimitowana liczba użytkowników Gwarancja min. 2 lata

1. Sprzęt dostarczony w ramach realizacji zamówienia musi być fabrycznie nowy, wyprodukowany nie wcześniej niż na 6 miesięcy od daty dostarczenia.
2. Sprzęt dostarczony w ramach realizacji zamówienia będzie pochodzić z autoryzowanego kanału sprzedaży producentów zaoferowanych urządzeń.
3. Sprzęt dostarczony w ramach realizacji zamówienia nie był w dniu składania ofert przeznaczony przez producenta do wycofania z produkcji.
4. Wraz z dostawą urządzenia Wykonawca dostarczy dokument wystawiony przez producenta sprzętu potwierdzający, że oprogramowanie w nim zawarte jest licencjonowane na Zamawiającego.

5. Wraz z dostawą sprzętu Wykonawca dostarczy szczegółową dokumentację techniczną producenta oferowanego urządzenia, potwierdzającą spełnianie wymagań technicznych sprzętu będącego przedmiotem zamówienia.

Szkolenie urzędników z zakresu cyberbezpieczeństwa

Szkolenie z zakresu cyberbezpieczeństwa ma na celu podniesienie kompetencji kadry urzędniczej w obszarze zagrożeń teleinformatycznych, podniesienie poziomu bezpieczeństwa informacyjnego w Urzędzie, poznanie prawidłowej reakcji na cyberataki, podniesienie świadomości w zakresie potencjalnych cyberryzyk oraz incydentów, unikanie nieświadomego naruszenia bezpieczeństwa informacji podczas pracy zdalnej, poznanie podstawowych zasad i dobrych praktyk wykorzystania technologii informatycznych oraz zdobycie umiejętności wykorzystania tej wiedzy w praktyce. Szkolenie w swym zakresie winno obejmować co najmniej następujące zagadnienia:

1. Omówienie poprawnych zasad związanych z cyberbezpieczeństwem w Urzędzie, w szczególności wynikających z obowiązujących w tym zakresie aktów prawnych (Ustawa o krajowym systemie cyberbezpieczeństwa, Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności i inne).
2. Szczegółowe informacje związane z zagrożeniami w sieci, w szczególności: phishing, ransomware oraz malware i omówienie sposobów przeciwdziałania oraz zabezpieczenia się przed powyższym zagrożeniami.

Wykonawca w ramach usługi przeprowadzi szkolenie dla 20 urzędników z Urzędu Gminy w Szreńsku. Przed realizacją usługi przygotuje harmonogram szkolenia oraz jego program i dostarczy je w terminie nie później niż 7 dni przed planowanym dniem rozpoczęcia szkolenia do akceptacji przez Zamawiającego. Szkolenie odbyć się musi w formie stacjonarnej w siedzibie Zamawiającego. Zamawiający udostępni pomieszczenie umożliwiające przeprowadzenie szkolenia w grupach maksymalnie 10 osobowych.

Wykonawca przygotuje i zapewni wszystkim uczestnikom najpóźniej w dniu szkolenia materiały szkoleniowe pozwalające na samodzielną edukację z zakresu tematyki szkolenia (np. opracowania, wydruki materiałów szkoleniowych). Dopuszczalne jest dostarczenie tych materiałów w formie elektronicznej np. plików w formacie PDF. Koszty związane z przygotowaniem i dostarczeniem materiałów szkoleniowych ponosi Wykonawca.

Wykonawca jest zobowiązany do zapewnienia uczestnikom możliwości konsultacji bezpośrednio po ukończeniu szkolenia, a także wskaże adres mailowy na który w ciągu 7 dni od ukończenia szkolenia uczestnicy będą mogli kierować pytania oraz udzieli na nie odpowiedzi w terminie nie późniejszym niż 10 dni od ukończenia szkolenia.

Szkolenie musi być certyfikowane. Wykonawca w ramach realizacji Zamówienia zapewni uczestnikom szkolenia imienne certyfikaty potwierdzające ukończenie szkolenia ze wskazaniem jego zakresu.