Załącznik nr 1 do zapytania ofertowego - OPZ

Opis Przedmiotu Zamówienia

Na potrzeby zapytania ofertowego prowadzonego w trybie zapytania ofertowego, zwanego dalej Zapytaniem, do którego nie mają zastosowania przepisy Ustawy z dnia 11 września 2019 r.- Prawo zamówień publicznych., zwanej dalej „ustawą Pzp".

Opis ogólny:

Przedmiotem zamówienia jest organizacja praktycznego **specjalistycznego szkolenia stacjonarnego dla administratorów IT i pracowników technicznych urzędu oraz jednostek podległych,** które potrwa dwa dni (po min. 5 godzin dziennie), dotyczącego prawidłowej konfiguracji oraz zabezpieczania kluczowych elementów infrastruktury sieciowej w jednostce samorządu terytorialnego.

Program szkolenia obejmuje trzy zasadnicze zagadnienia: serwerowy system operacyjny, urządzenie UTM oraz przełączniki sieciowe, a dodatkowo ma uwzględniać kwestie ogólnego bezpieczeństwa sieci UG, z naciskiem na identyfikację i minimalizację potencjalnych zagrożeń.

Zakres szkolenia

a) Konfiguracja i zabezpieczenie serwera – 1 dzień, 1 uczestnik

- Omówienie podstawowych i zaawansowanych ról serwera, w tym usług sieciowych (np. DNS, DHCP), wraz z zaleceniami dotyczącymi ochrony przed nieuprawnionym dostępem
- Zasady tworzenia kopii zapasowych, sposoby odzyskiwania danych i scenariusze reagowania na awarie (np. w przypadku błędów dyskowych lub ataków typu ransomware)
- Ustalanie polityk haseł, uwierzytelnianie użytkowników i rola ograniczenia uprawnień administracyjnych (poziom minimalnych przywilejów)
- Metody logowania zdarzeń i analizy dzienników (logów), uwzględniające szybką identyfikację nieprawidłowości oraz nieautoryzowanych prób wejścia do systemu

b) UTM – uniwersalna ochrona brzegu sieci – 1 dzień, 1 uczestnik

- Zasada działania urządzeń UTM (Unified Threat Management) i znaczenie wielowarstwowej ochrony na styku z siecią zewnętrzną
- Konfiguracja reguł firewall i filtrowania ruchu, przygotowywanie profili bezpieczeństwa (np. do blokowania niechcianych portów, przesyłania złośliwych plików)

CENTRUM PROJEKTÓW POLSKA CYFROWA
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.pl

- Wydzielanie stref za pomocą wirtualnych sieci (VLAN) i ich obsługa w urządzeniu UTM, co wspomaga segmentację ruchu i redukuje możliwość poruszania się atakującego w przypadku naruszenia jednej strefy
- Tworzenie bezpiecznych połączeń zdalnych z użyciem protokołów VPN, pozwalających na szyfrowanie transmisji oraz uwierzytelnianie użytkowników

c) Przełączniki sieciowe i segmentacja LAN – 1 dzień, 1 uczestnik

- Znaczenie konfigurowania sieci VLAN w celu podniesienia bezpieczeństwa i odizolowania wybranych grup urządzeń lub użytkowników
- Szczegółowa konfiguracja przełączników (switche L2/L3), z uwzględnieniem trunków, portów dostępowych (access) i mechanizmów zapobiegających pętlom (Spanning Tree)
- Dobre praktyki w zakresie zabezpieczenia portów, blokowania nieużywanych interfejsów i ograniczania możliwości wykonywania ataków od strony sieci lokalnej (np. ARP spoofing)
- Sposoby monitorowania stanu przełącznika, analiza tablic MAC oraz reagowanie na próby nieuprawnionego przełączenia urządzeń

d) Ogólne bezpieczeństwo sieci JST – 2 dzień, 5 Uczestników

- Wyjaśnienie, w jaki sposób Gmina może całościowo chronić swoje zasoby, biorąc pod uwagę różnorodność działów i pracowników
- Omówienie procedury przyznawania i odbierania uprawnień, tak aby zredukować ryzyko nadużyć wewnętrznych, zwłaszcza w połączeniu z niewystarczającą segmentacją VLAN
- Przedstawienie procesów zarządzania aktualizacjami (systemowymi i firmware), w tym okresowe przeglądy stanu zabezpieczeń oraz identyfikowanie nowo wykrytych podatności
- Przykłady typowych ataków spotykanych w administracji samorządowej (phishing ukierunkowany, socjotechnika przez telefon, przejęcie dostępu do kont uprzywilejowanych) wraz z zaleceniami, jak na nie reagować
- Szkolenie obejmie także znaczenie edukacji użytkowników w Gminie, by rozumieli wagę stosowania silnych haseł, unikania podejrzanych linków i raportowania wszelkich podejrzanych incydentów

Organizacja szkolenia

- Łączny czas trwania zajęć to min. dwie sesje, po min. 5 godzin każda, co umożliwia omówienie najważniejszych zagadnień oraz przeprowadzenie podstawowych ćwiczeń praktycznych.
- Szkolenie odbędzie się na terenie UG w odpowiednio przystosowanej sali, pozwalającej na prezentację krok po kroku, jak konfigurować i zabezpieczać kluczowe elementy infrastruktury
- Zakres tematyczny należy tak ułożyć, by uwzględniał zróżnicowany poziom wiedzy słuchaczy, przy czym przynajmniej połowa szkolenia będzie mieć formę warsztatu na bazie sprzętu posiadanego przez UG.
- Zostaną udostępnione materiały cyfrowe ze szkolenia „Ogólne bezpieczeństwo sieci JST – 2 dzień” umożliwiające zapoznanie się z nimi uczestnikom poza terminem szkolenia.

Rezultaty szkolenia

- Po zakończeniu zajęć uczestnicy będą potrafili:
  a) Samodzielnie konfigurować usługi serwerowe z uwzględnieniem bezpieczeństwa i zapobiegania awariom
  b) Wdrażać skuteczne reguły i polityki w urządzeniach UTM, z naciskiem na kontrolę ruchu oraz bezpieczne łączenie sieci VLAN
  c) Organizować przełączniki w topologii VLAN i prawidłowo segmentować ruch, by ograniczyć rozprzestrzenianie się potencjalnego ataku i łatwiej monitorować aktywność w sieci
  d) Rozumieć koncepcję ogólnego bezpieczeństwa w strukturze Gminy, co oznacza regularne przeglądy zabezpieczeń, aktualizacje i świadome reagowanie na nietypowe zdarzenia

Wymagania wobec Wykonawcy

- Wykonawca powinien mieć doświadczenie w administrowaniu serwerami, urządzeniami UTM oraz przełącznikami sieciowymi, w tym potrafić przedstawić realne przykłady i demonstracje
- Wykonawca posiada następujące certyfikaty potwierdzające posiadaną wiedzę oraz doświadczenie:

a) Min. 1 jeden certyfikat potwierdzający praktyczne umiejętności w zakresie administracji i konfiguracji serwerowych systemów operacyjnych, w tym obsługę usług sieciowych oraz mechanizmów zabezpieczeń.
b) Min. 1 jeden certyfikat potwierdzający kompetencje w obszarze zaawansowanej konfiguracji i zarządzania infrastrukturą sieciową (routing, firewall, rozbudowane mechanizmy trasowania i filtrowania ruchu).
c) Min. 1 jeden certyfikat w zakresie obsługi i utrzymania środowisk pamięci masowej klasy korporacyjnej, obejmujący zarządzanie wolumenami, tworzenie i przydzielanie zasobów oraz zapewnianie redundancji i bezpieczeństwa danych.

Dokumentacja i rozliczenie

- Wykonawca zapewni uczestnikom materiały szkoleniowe (w formie elektronicznej lub papierowej), obejmujące najważniejsze procedury konfiguracyjne i rekomendowane rozwiązania
- Po zakończeniu szkolenia sporządzony zostanie protokół odbioru, potwierdzający zrealizowanie wskazanego zakresu.
- Każdy uczestnik szkolenia otrzyma stosowny certyfikat z wyszczególnieniem zakresu pozyskanej i sprawdzonej wiedzy.
- Rozliczenie finansowe nastąpi po podpisaniu protokołu odbioru przez Zamawiającego i Wykonawcę

Postanowienia końcowe

- **Termin realizacji szkolenia to okres od 10.08.2026 do 21.08.2026 r.** Termin szkolenia zostanie ustalony z Zamawiającym, tak aby pracownicy JST mogli zaplanować udział w warsztatach, nie zaburzając ciągłości pracy urzędu i innych jednostek.
- W ramach umowy Wykonawca zobowiązuje się do przekazania ewentualnych poprawek i aktualizacji materiałów (np. jeśli pojawią się nowe wytyczne dotyczące zabezpieczeń) przez 6 miesięcy po zakończeniu szkolenia.
- Wszelkie dodatkowe ustalenia, takie jak szczególne wymagania sprzętowe lub preferowany podział tematyczny, zostaną ujęte w umowie lub aneksach, w zależności od potrzeb Zamawiającego.