Numer sprawy: **RIDiGP.271.1.9.2024.ZP Załącznik numer 6a do SWZ**

**Zadanie nr 1**

Spis treści

[1 SZKOLENIE DLA DZIAŁU IT (szkolenie dot. UTM). 2](#_Toc179374389)

[2 SZKOLENIE DLA DZIAŁU IT (szkolenie Microsoft Active Directory) 3](#_Toc179374390)

[3 SZKOLENIE DLA PRACOWNIKÓW SPOZA DZIAŁU IT (cyberbezpieczeństwo). 5](#_Toc179374391)

## 1 SZKOLENIE DLA DZIAŁU IT (szkolenie dot. UTM).

|  |  |  |  |
| --- | --- | --- | --- |
| L.P | Nazwa | **Minimalne wymagania dla szkolenia** | **Oferowane parametry** |
|  |  | Zamówienie będzie realizowane na rzecz **Urzędu Gminy Rogowo.** |  |
|  | Typ | Szkolenie z zakresu urządzenia klasy UTM wdrażanego w ramach projektu (Cześć I Obszar techniczny, pkt. 1. UTM Unified Threat Management: wznowienie supportu dla Urzędu Gminy w Rogowie oraz pkt. 2. UTM Unified Threat Management: urządzenie klasy UTM dla Ośrodka Pomocy Społecznej w Rogowie, 2 osoby formuła online. | SPEŁNIA TAK /NIE |
|  | Czas trwania | Minimum 3 dni (1 dzień = 8 godzin roboczych  3 dni =24 godziny robocze) | SPEŁNIA TAK /NIE |
|  | Lokalizacja | Szkolenie online | SPEŁNIA TAK /NIE |
|  | Wymagany minimalny zakres tematyczny | • Architektura urządzeń producenta,  • Wirtualizacja w obrębie urządzenia  • Wstępna konfiguracja urządzenia,  • Zaawansowania konfiguracja sieci i routingu  • Uwierzytelnianie użytkowników  • Tworzenie reguł firewall w oparciu o grupy użytkowników  • Dwuskładnikowa autoryzacja  • Wirtualne sieci prywatne- VPN  • Diagnostyka i rozwiązywanie problemów  • Konfiguracja urządzeń do pracy w klastrze HA | SPEŁNIA TAK /NIE |
|  | Trenerzy | Certyfikowani przez producenta rozwiązania. | SPEŁNIA TAK /NIE |
| 6. | Materiały szkoleniowe | Materiały elektroniczne | SPEŁNIA TAK /NIE |
| 7. | Ilość | 2 szt. | SPEŁNIA TAK /NIE |

## 2 SZKOLENIE DLA DZIAŁU IT (szkolenie Microsoft Active Directory)

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne) Oferowane parametry** | **Oferowane parametry** |
|  |  | Zamówienie będzie realizowane na rzecz **Urzędu Gminy Rogowo.** |  |
|  | Typ | Szkolenie dla działu IT dotyczące usługi katalogowej systemów Windows Server (Microsoft Active Directory) dla Urzędu Gminy w Rogowie dla 2 osób, formuła online. | SPEŁNIA TAK /NIE |
|  | Czas trwania | Minimum 2 dni tj.: (1 dzień = 8 godzin roboczych  2 dni =16 godzin roboczych) | SPEŁNIA TAK /NIE |
|  | Lokalizacja | Szkolenie online | SPEŁNIA TAK /NIE |
|  | Wymagany minimalny zakres tematyczny | Szkolenie musi zawierać co najmniej poniższe zagadnienia:   * Instalacja i konfiguracja kontrolerów domeny   + Omówienie usług Active Directory Domain Services   + Omówienie kontrolerów domeny usług AD DS   + Wdrożenie kontrolera domeny   + Omówienie usługi Encrypted DNS * Zarządzanie obiektami w Active Directory Domain Services   + Zarządzanie kontami użytkowników   + Zarządzanie grupami w usługach AD DS   + Zarządzanie obiektami typu komputer w AD DS   + Wdrażanie i zarządzanie jednostek organizacyjnych w AD DS * Zarządzanie zaawansowaną infrastrukturą Active Directory Domain Services * Wprowadzenie do zaawansowanych wdrożeń AD DS * Wdrożenie rozproszonego środowiska AD DS * Konfiguracja relacji zaufania AD DS. * Wdrażanie i zarządzanie lokacjami i repliką Active Directory Domain Services * Omówienie replikacji usług AD DS. * Konfigurowanie lokacji usług AD DS. * Konfigurowanie i monitorowanie replikacji usług AD DS. * Wdrażanie zasad grupy * Wprowadzenie do zasad grupy * Wdrażanie i zarządzanie obiektami GPO (Group Policy Object) * Konfiguracja zakresu przetwarzania obiektów GPO * Rozwiazywanie problemów GPO * Zarządzanie ustawieniami użytkowników za pomocą zasad grupy * Wdrażanie szablonów administracyjnych * Konfiguracja przekierowania folderów, instalacji oprogramowania i skryptów   Konfiguracja preferencji zasad grupowych | SPEŁNIA TAK /NIE |
|  | Trenerzy | Trenerzy prowadzący szkolenie muszą posiadać certyfikat producenta rozwiązania. | SPEŁNIA TAK /NIE |
|  | Materiały szkoleniowe | Materiały elektroniczne | SPEŁNIA TAK /NIE |
|  | Wsparcie trenera po szkoleniu | Co najmniej 14 dni | SPEŁNIA TAK /NIE |
|  | Ilość | 2 szt. | SPEŁNIA TAK /NIE |

## 3 SZKOLENIE DLA PRACOWNIKÓW SPOZA DZIAŁU IT (cyberbezpieczeństwo).

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
|  |  | Zamówienie będzie realizowane na rzecz **Urzędu Gminy Rogowo.** |  |
|  | Typ | Szkolenie dla pracowników spoza działu IT (cyberbezpieczeństwo)- szkolenie dla pracowników Urzędu Gminy (1 grupa, 30 osób, szkolenie online). | SPEŁNIA TAK /NIE |
|  | Przygotowanie i przeprowadzenie kampanii phishingowej | Zakres i planowany przebieg Testów phishingowych (TP) w zakresie minimum:   1. Zamawiający wymaga ustalenia scenariusza w zakresie minimum: Opracowania i zatwierdzenie z Zamawiającym szczegółowego scenariusza ataku socjotechnicznego. Wyboru metod i narzędzi do jego realizacji.  Szczegóły kampanii, w tym scenariusze socjotechniczne oraz harmonogram realizacji, muszą zostać ustalone i zatwierdzone przez Zamawiającego co najmniej 14 dni przed planowanym rozpoczęciem kampanii. 2. Zamawiający wymaga przeprowadzenia przygotowań ataku w zakresie minimum:  * Projektowanie minimum 1 szablonu mailowych * Przygotowanie minimum 1 fałszywej domeny i konfiguracja hostingu. * Listy odbiorców * Finalizacja listy docelowych odbiorców w oparciu o informacje uzyskane od Zamawiającego.  1. Zamawiający wymaga przeprowadzenie startu realizacji ataku w zakresie minimum:  * Rozpoczęcie kampanii phishingowej: * Kampania musi zostać przeprowadzona w ciągu minimum 3 dni, rozpoczynając się od wysyłki mailowej do wybranych odbiorców.  1. Zamawiający wymaga kontynuacji kampanii i monitorowania w zakresie minimum:  * Dostosowania harmonogramu wysyłki do ustaleń przeprowadzonych z  Zamawiającym na etapie ustalania scenariusza. * Czas trwania kampanii od min 3 dni roboczych zostaje dostosowana w oparciu o ustalenia z Zamawiającym przeprowadzone podczas pierwszego etapu – Ustalenie scenariusza. * Kampania powinna być realizowana etapami, z wysyłkami dokonywanymi w określonych partiach i godzinach, aby zapewnić maksymalną skuteczność. * Monitorowanie reakcji pracowników urzędu * Bieżące śledzenie odpowiedzi i interakcji odbiorców z wysłanymi wiadomościami * Analiza efektywności i w razie potrzeby, wprowadzanie zmian w strategii kampanii.  1. Zamawiający wymaga przeprowadzenia zakończenia kampanii i przygotowanie raportu w zakresie minimum:  * Zakończenie wysyłki mailowej- przedstawienie efektów * Zebranie i dokonanie pierwszej analizy zebranych danych na temat interakcji i reakcji na przeprowadzone działania. * Przygotowania raportu końcowego dotyczącego skuteczności kampanii, zawierającego wszystkie zebrane dane, zakresie minimum:  1. Opis wykorzystanych i skonfigurowanych domen 2. Opis szablonów oraz opis celu jaki stanowi podczas realizacji kampanii 3. Opis niebezpieczeństw związanych z dalszymi krokami prawdziwego ataku 4. Statystyki kampanii phishingowej, w tym: liczby wysłanych, otwartych maili, liczby kliknięć w link, liczby osób, które podały swoje dane. 5. Podsumowanie oraz rekomendacje | SPEŁNIA TAK /NIE |
|  | Szkolenie z cyberbezpieczeństwa | Szkolenie musi zostać przeprowadzone w jednej grupie liczącej maksymalnie 30 osób. Szkolenie online trwające minimum 1 godzinę.  Szkolenie musi obejmować w zakresie minimum:   * Wycieki informacji – mechanizmy i skutki. * Zarządzanie hasłami – dobre praktyki i narzędzia pomocnicze. * Psychomanipulacja w sieci – zasady i zastosowania. * Sfałszowane komunikaty i strony – identyfikacja zagrożeń. * Ataki głosowe i podszywanie się pod identyfikator dzwoniącego (vishing) * Archiwizacja internetowa – cyfrowy ślad nie znika. * Mechanizmy śledzenia w sieci – rola i funkcja cookies. * Niebezpieczeństwa ze strony nieautoryzowanego sprzętu. * Ataki siłowe na hasła – jak nie dać się złamać. * Wyłudzenie informacji przez celowane ataki phishingowe (spear phishing). * Świadomość pracowników – kultura bezpieczeństwa w organizacji. | SPEŁNIA TAK /NIE |
|  | Ilość | 1 szt. | SPEŁNIA TAK /NIE |