**Załącznik nr 6.2 do SWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

1. Pakiet szkoleń dla informatyka

Ilość: 1 pakiet

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry techniczne** |
| Szkolenie dla Administaratora z istniejącego urządzenia UTM | Autoryzowane szkolenie z urządzenia UTM. Zakres podstawowy:   1. Rozpoczęcie pracy z urządzeniem    * Rejestracja w strefie klienta i dostęp zasobów    * Rozpoczęcie pracy z urządzeniem i wprowadzenie do interfejsu administracyjnego    * Ustawienia systemowe i uprawnienia administratorów    * Instalacja licencji i aktualizacja systemu    * Tworzenie kopii zapasowej i przywracanie konfiguracji 2. Zbieranie logów i monitorowanie    * Przedstawienie kategorii zbieranych logów    * Wykresy historyczne i monitorowanie 3. Obiekty    * Typy obiektów oraz ich wykorzystanie    * Obiekty sieciowe i obiekt typu „router” 4. Konfiguracja sieci    * Tryby pracy urządzenia    * Typyinterfejsów (Ethernet, modem, bridge, VLAN, GRETAP)    * Typy routingu oraz ich priorytety 5. Translacja adresów sieciowych (NAT) 6. Translacja połączeń wychodzących (maskarada) 7. Translacja połączeń przychodzących (przekierowanie) 8. Translacja dwukierunkowa (jeden do jeden) 9. Filtrowanie ruchu sieciowego (Firewall) 10. Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (Statefulinspection)     * Szczegółowy opis parametrów reguły Firewall     * Kolejność przetwarzania reguł Firewall i NAT 11. Ochrona aplikacji     * Implementacja filtrowania URL dla ruchu http i https     * Konfigurowanie skanowania antywirusowego i modułu Breach Fighter     * Moduł IPS i stosowanie profili inspekcji 12. Użytkownicy i uwierzytelnianie 13. Konfiguracja usługi katalogowej     * Wprowadzenie do różnych metod uwierzytelniania (LDAP, Kerberos, Radius, certyfikat SSL, SPNEGO, SSO)     * Rejestracja użytkowników     * Uwierzytelnianie użytkowników za pomocą portalu uwierzytelniania 14. Wirtualne sieci prywatne (VPN)     * Koncepcje i ogólne informacje dotyczące protokołu IPSec VPN (IKEv1 i IKEv2)     * Tunele Site-to-Site z wykorzystaniem klucza współdzielonego (PSK)     * Tunele VTI 15. SSL VPN     * Zasada działania     * Konfiguracja   Szkolenie online min. 24h  Zakres rozszerzony:   1. Szczegółowe omówienie działania modułu IPS    * Różnice pomiędzy IPS a IDS    * moduł IPS    * Różne tryby analizy    * Profile oparte na protokołach i aplikacjach 2. Infrastruktura klucza publicznego    * Podstawy szyfrowania symetryczneg - i asymetrycznego    * Typy szyfrowania    * Infrastruktura klucza publiczneg    * Tworzenie urzędu certyfikacji, certyfikatów serwera i użytkowników 3. SSL Proxy    * Zasada działania    * Konfiguracja SSL Proxy    * Zaawansowana konfiguracja tuneli IPSec VPN    * Szczegółowy opis działania mechanizmu NAT traversal    * Obsługa funkcji DPD (Dead Peer Detection)    * Architektura sieci VPN typu „gwiazda” i „mesh”    * NAT w sieciach IPSec VPN    * Konfiguracja zapasoweg - tunelu IPSec VPN    * Konfiguracja tuneli Site-to-Site w oparciu - certyfikaty    * Konfiguracja tuneli dla użytkowników mobilnych (Client-2-Site) 4. GRE i GRETAP    * Zasada działania    * Konfiguracja i instalacja 5. Transparentne uwierzytelnianie użytkowników    * Zasada działania    * Metoda uwierzytelniania SPNEGO    * Metoda uwierzytelniania oparta na certyfikatach SSL 6. Wysoka dostępność (HA)    * Zasada działania    * Kreator umożliwiający tworzenie i konfigurowanie klastra HA    * Konfiguracja interfejsu sieciowego    * Zaawansowana konfiguracja   Szkolenie online min. 24h  Możliwość otrzymania certyfikatu po zdaniu egzaminu  Możliwość dostawy vouchera szkoleniowego z terminem ważności min. 1 rok. |  |
| **Szkolenie z dostarczonego systemu operacyjnego w serwerach** | Autoryzowane szkolenie producenta z dostarczonego systemu operacyjnego w serwerze. Zakres szkolenia:  Moduł  1. Instalowanie i konfigurowanie kontrolerów domeny  2. Zarządzanie obiektami w usługach AD DS  3. Zarządzanie zaawansowaną infrastrukturą AD DS  4. Implementowanie lokacji usług AD DS oraz konfigurowanie replikacji i zarządzanie nią  5. Wdrażanie zasad grupy  6. Zarządzanie ustawieniami użytkownika za pomocą zasad grupy  7. Zabezpieczanie usług domenowych Active Directory  8. Wdrażanie usług AD CS i zarządzanie nimi  9. Wdrażanie certyfikatów i zarządzanie nimi  10. Wdrażanie i administrowanie usługami AD FS  11. Wdrażanie i administrowanie usługi AD RMS  12. Monitorowanie usług AD DS, zarządzanie nimi oraz odzyskiwanie danych  Szkolenie online min. 40h  Certyfikat ukończenia szkolenia  Możliwość dostawy vouchera szkoleniowego z terminem ważności min. 1 rok. |  |
| **Szkolenie z backupu** | Szkolenie z backupu min. 4 godzin obejmujące następujące zagadnienia:  Wprowadzenie do backupu  Instalacja oprogramowania  Funkcje oprogramowania  Ustawienie backupu  Odzyskiwanie danych  Możliwość dostawy vouchera szkoleniowego z terminem ważności min. 1 rok. |  |

1. Szkolenia dla pracowników

Ilość: 1 pakiet

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry techniczne** |
| **Opis** | Zakres szkolenia:   1. **Główne założenia i wymagania prawne dotyczące cyberbezpieczeństwa w pracy urzędnika.**     * 1. Czym jest cyberbezpieczeństwo      2. Od czego zależy bezpieczeństwo informacji      3. Obowiązki Jednostek samorządu terytorialnego wynikające z obowiązujących aktów prawnych związanych z bezpieczeństwem informacji 2. **Przegląd najpopularniejszych zagrożeń oraz zasady bezpiecznego korzystania z internetu)** 3. Czym są ataki socjotechniczne 4. Rodzajeataków (phishing ,spearphishing, vishing, smishing, quishing) 5. Jak rozpoznać atak 6. Jakie dane chcą pozyskać przestępcy 7. Jak uniknąć zagrożenia 8. Przydatne narzędzia 9. **Bezpieczeństwo fizyczne w ochronie informacji.** 10. Regulacje i zasady, które należy stosować w biurze 11. Fizyczne metody ochrony informacji 12. Ochrona nośników informacji 13. Bezpieczna praca poza biurem 14. **Bezpieczeństwo haseł** 15. Statystyki ataków na hasła 16. Hasła w upublicznionych wyciekach 17. Zasady tworzenia silnych haseł 18. Metody ochrony haseł 19. **Bezpieczne korzystanie z witryn internetowych** 20. Na co zwrócić uwagę przed otwarciem witryny 21. Najnowsze przykłady fałszywych witryn 22. Jak się chronić 23. **Przegląd znanych typów ataków na samorządy.** 24. Ransomware i inne rodzaje ataków najczęściej kierowane na JST 25. Skutki ataków dla JST 26. Jak się chronić przed atakami   Szkolenie na miejscu w siedzibie Zamawiającego.  Ilość osób do przeszkolenia: min. 16 osób  Ilość grup: min. 2  Ilość osób w grupie: max. 8 osób  Czas szkolenia 1 grupy: min. 3 h  Dyplom potwierdzający ukończenia szkolenia. |  |

1. Szkolenia dla kadry zarządzającej

Ilość: 1 pakiet

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry techniczne** |
| **Opis** | Zakres szkolenia:   1. **Główne założenia i wymagania prawne dotyczące cyberbezpieczeństwa w pracy urzędnika.** 2. Czym jest cyberbezpieczeństwo 3. Od czego zależy bezpieczeństwo informacji 4. Obowiązki Jednostek samorządu terytorialnego wynikające z obowiązujących aktów prawnych związanych z bezpieczeństwem informacji 5. **Przegląd najpopularniejszych zagrożeń oraz zasady bezpiecznego korzystania z internetu)** 6. Czym są ataki socjotechniczne 7. Rodzajeataków (phishing ,spearphishing, vishing, smishing, quishing) 8. Jak rozpoznać atak 9. Jakie dane chcą pozyskać przestępcy 10. Jak uniknąć zagrożenia 11. Przydatne narzędzia 12. **Bezpieczeństwo fizyczne w ochronie informacji.** 13. Regulacje i zasady, które należy stosować w biurze 14. Fizyczne metody ochrony informacji 15. Ochrona nośników informacji 16. Bezpieczna praca poza biurem 17. **Bezpieczeństwo haseł** 18. Statystyki ataków na hasła 19. Hasła w upublicznionych wyciekach 20. Zasady tworzenia silnych haseł 21. Metody ochrony haseł 22. **Bezpieczne korzystanie z witryn internetowych** 23. Na co zwrócić uwagę przed otwarciem witryny 24. Najnowsze przykłady fałszywych witryn 25. Jak się chronić 26. **Przegląd znanych typów ataków na samorządy.** 27. Ransomware i inne rodzaje ataków najczęściej kierowane na JST 28. Skutki ataków dla JST 29. Jak się chronić przed atakami 30. **Moduł dla kadry zarządzającej.** 31. System Zarządzania Bezpieczeństwem Informacji oparty o normę ISO 27001:2023 - wymagania i procedury 32. Zarządzanie ryzykiem w bezpieczeństwie informacji 33. Ciągłość działania – wymagania oparte na normie ISO 22301 34. Zarządzanie incydentem w urzędzie   Szkolenie na miejscu w siedzibie Zamawiającego.  Ilość osób do przeszkolenia: min. 4 osób  Ilość grup: min. 1  Ilość osób w grupie: max. 4 osób  Czas szkolenia 1 grupy: min. 4 h  Dyplom potwierdzający ukończenia szkolenia. |  |