OPIS PRZEDMIOTU ZAMÓWIENIA

Rozdział I. Określenie przedmiotu zamówienia

Nazwa zamówienia: „Szkolenia z zakresu cyberbezpieczeństwa".

Przedmiot zamówienia jest realizowany w ramach zadania budżetowego „Cyberbezpieczny Powiat Zduńskowolski".

Projekt „Cyberbezpieczny Powiat Zduńskowolski" jest dofinansowany ze środków europejskich i budżetu państwa w ramach konkursu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23 (Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa).

Zamówienie zostało podzielone dwie części:

Część 1. Pakiet szkoleń specjalistycznych w zakresie zastosowanych środków bezpieczeństwa w ramach projektu grantowego „Cyberbezpieczny Powiat Zduńskowolski" dla 3 pracowników IT Starostwa Powiatowego w Zduńskiej Woli.

Część 2. Pakiet szkoleń podstawowych, budujących świadomość cyberzagrożeń i sposobów ochrony dla 112 pracowników Starostwa Powiatowego w Zduńskiej Woli i Powiatowego Centrum Pomocy Rodzinie w Zduńskiej Woli.

Rozdział II. Wymagania ogólne

W obu częściach zamówienia muszą zostać zachowane zasady równości szans i niedyskryminacji, w tym dostępności dla osób z niepełnosprawnościami oraz równości kobiet i mężczyzn.

Obie części zamówienia muszą zostać zrealizowane z uwzględnieniem obowiązujących przepisów prawa, w tym w szczególności:

1. Rozporządzeniem Parlamentu Europejskiego i Rady (EU) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
2. Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
3. Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
4. Dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/255 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).

Wszystkie opracowane materiały szkoleniowe, zaświadczenia o ukończeniu szkoleń, listy obecności, listy odbioru zaświadczeń o ukończeniu szkolenia muszą zawierać informację o współfinansowaniu projektu ze środków Unii Europejskiej w ramach grantu „Cyberbezpieczny samorząd” oraz logotypy według wzoru przekazanego przez Zamawiającego.

Rozdział III. Wymagania szczegółowe

III.1. Wymagania szczegółowe w zakresie Części 1

Część 1 obejmuje pakiet szkoleń specjalistycznych w zakresie zastosowanych środków bezpieczeństwa w ramach projektu grantowego „Cyberbezpieczny Powiat Zduńskowolski" dla trzech pracowników IT Starostwa Powiatowego w Zduńskiej Woli oraz Powiatowego Centrum Pomocy Rodzinie w Zduńskiej Woli, w zakresie której należy zrealizować następujące szkolenia:

1. **Szkolenie: administracja urządzeniami Fortinet**
   - **1.1. Cel usługi szkoleniowej**: zdobycie przez uczestników szkolenia praktycznych umiejętności w zakresie konfigurowania i administrowania posiadanych/posiadanymi przez Zamawiającego urządzeń/urządzeniami Fortinet: FortiGate, FortiAnalyzer, FortiAP, FortiSwitch (urządzeniami Zamawiającego). Uczestnicy szkolenia muszą uzyskać wiedzę i umiejętności umożliwiające efektywne, sprawne, skuteczne i bezpieczne konfigurowanie, użytkowanie oraz zarządzanie ww. urządzeniami.
   - **1.2. Wymóg autoryzacji szkolenia przez producenta rozwiązania** z uwagi:
     - 1.2.1. na charakter usługi szkoleniowej oraz jej ww. cel, oraz związaną z nią potrzebę zapewnienia pełnej użyteczności wiedzy i umiejętności nabytych przez uczestników szkolenia;
     - 1.2.2. na to, że jakość i zakres usługi szkoleniowej oraz zdobyte dzięki uczestnictwie w szkoleniu wiedza i umiejętności będą wpływać bezpośrednio na poziom cyberbezpieczeństwa Zamawiającego.

     Zamawiający zastrzega, że szkolenie/szkolenie równoważne musi być autoryzowane przez producenta posiadanych przez Zamawiającego urządzeń FortiGate.
   - **1.3. Forma szkolenia**: szkolenie realizowane stacjonarnie w siedzibie Zamawiającego.
   - **1.4. Język prowadzenia szkolenia**: szkolenie zostanie przeprowadzone w języku polskim.
   - **1.5. Liczba uczestników szkolenia** (liczba szkolonych osób): 3 osoby (pracownicy działów IT Zamawiającego).
   - **1.6. Czas trwania szkolenia** – szkolenie zostanie zrealizowane w następującym wymiarze:
     - 1.6.1. liczba dni: minimum 4;
     - 1.6.2. liczba godzin: minimum 24 godziny, w tym minimum 10 godzin laboratoriów (zajęć praktycznych).
   - **1.7. Termin szkolenia, harmonogram oraz program szkolenia**.
     - 1.7.1. szkolenia powinny się odbyć w terminie 6 miesięcy od dnia podpisania umowy;
     - 1.7.2. Wykonawca w ramach wykonania usługi szkoleniowej przygotuje harmonogram i program szkolenia i dostarczy go do akceptacji Zamawiającego w terminie do czternastu dni od daty zawarcia umowy.
   - **1.8. Materiały szkoleniowe**
     - 1.8.1. każdy uczestnik szkolenia otrzyma w pierwszym dniu szkolenia dostęp do materiałów szkoleniowych w postaci elektronicznej;
     - 1.8.2. materiały szkoleniowe muszą obejmować cały zakres merytoryczny szkolenia;
     - 1.8.3. materiały szkoleniowe zostaną przygotowane i sporządzone w języku polskim;
     - 1.8.4. wszelkie koszty materiałów szkoleniowych ponosi Wykonawca.
   - **1.9. Zakres merytoryczny szkolenia.** Szkolenie do urządzeń Fortinet musi zawierać zagadnienia:
     - 1.9.1. Rejestracja urządzeń/omówienie panelu, konfiguracja kont
     - 1.9.2. Wstępna konfiguracja, omówienie trybów pracy Nat/Transparent
     - 1.9.3. Fortiguard:

1.9.3.1. konfiguracja aktualizacji
1.9.3.2. testowanie połączenia z usługą FortiGuard
1.9.4. FortiCloud, FortiSandbox Cloud – omówienie i konfiguracja
1.9.5. Podstawowe i zaawansowane funkcje Forti OS.
1.9.5.1. omówienie funkcji
1.9.5.2. włączanie / wyłączanie funkcji
1.9.6. Konfiguracja reguł zapory sieciowej
1.9.7. Konfiguracja przekierowania portów
1.9.8. Konfiguracja powiadomień dla użytkowników końcowych
1.9.9. Logowanie danych:
1.9.9.1. sposoby logowania danych
1.9.9.2. wyszukiwanie/filtrowanie logowanych zdarzeń
1.9.10. Obsługa kilu łączy (failover, load balancing)
1.9.11. VPN – omówienie i konfiguracja połączeń klienckich, oraz Site to Site
1.9.12. Integracja z domeną LDAP, omówienie Single Sign ON
1.9.13. Uwierzytelnienia dwuskładnikowe
1.9.14. Kontrola aplikacji
1.9.15. Konfiguracja AV
1.9.16. Konfiguracja IPS/IDS
1.9.17. Konfiguracja Webfiltering'u
1.9.18. Konfiguracja Antyspamu
1.9.19. Analiza ruchu szyfrowanego
1.9.20. Konfiguracja powiadomień o zdarzeniach (Alerty,Raporty)
1.9.21. Sposoby debugowania/analizy ruchu na urządzeniu.
1.9.22. Backup/przywracanie ustawień urządzenia,
1.9.23. Awaryjne zarządzanie urządzeniem.
1.9.24. Optymalizacja konfiguracji i monitorowania obciążenia systemu – dobre praktyki
1.9.25. Instalcja FortiAnalyzera, wstępna konfiguracja
1.9.26. Podłączenie urządzenia, dodanie FortiGate do FortiAnalyzera
1.9.27. LogView
1.9.28. FortiView
1.9.29. Omówienie FabricView
1.9.30. Raporty

1.10. **Trener realizujący usługę szkoleniową:** musi posiadać certyfikat wystawiony przez Producenta urządzeń Zamawiającego, to jest: certyfikat Fortinet Certified Trainer (FCT), a w przypadku zaoferowania szkolenia równoważnego: certyfikat wystawiony przez Producenta urządzenia równoważnego, uprawniający do prowadzenia szkoleń z zakresu konfigurowania i administrowania urządzenia równoważnego.

1.11. **Certyfikat ukończenia szkolenia**: po ukończeniu szkolenia, uczestnicy szkolenia otrzymują certyfikat ukończenia szkolenia sygnowany przez Producenta urządzeń Zamawiającego.

2. Szkolenie: Zarządzanie bazą danych SQL

2.1. Cel usługi szkoleniowej: Po ukończeniu szkolenia, uczestnik będzie potrafił: efektywnie zarządzać, zabezpieczać i optymalizować bazy danych SQL Server oraz Azure SQL, zapewniając ich wydajność i ciągłość działania.

2.2. Wymóg autoryzacji szkolenia przez Producenta rozwiązania z uwagi:

2.2.1. na charakter usługi szkoleniowej oraz jej ww. cel, oraz związaną z nią potrzebę zapewnienia pełnej użyteczności wiedzy i umiejętności nabytych przez uczestników szkolenia;

2.2.2. na to, że jakość i zakres usługi szkoleniowej oraz zdobyte dzięki uczestnictwie w szkoleniu wiedza i umiejętności będą wpływać bezpośrednio na poziom cyberbezpieczeństwa Zamawiającego;

Zamawiający zastrzega, że szkolenie/szkolenie równoważne musi być autoryzowane przez Producenta posiadanych przez Zamawiającego oprogramowania firmę: Microsoft.

2.3. Forma szkolenia: szkolenie realizowane stacjonarnie w siedzibie Zamawiającego.

2.4. Język prowadzenia szkolenia. szkolenie zostanie przeprowadzone w języku polskim.

2.5. Liczba uczestników szkolenia (liczba szkolonych osób): 3 osoby (pracownicy działu IT Zamawiającego).

2.6. Czas trwania szkolenia. Szkolenie zostanie zrealizowane w następującym wymiarze:

2.6.1. liczba dni: minimum 5 dni;

2.6.2. liczba godzin: minimum 40 godziny lekcyjnych, w tym minimum godzin laboratoriów (zajęć praktycznych).

2.7. Termin szkolenia, harmonogram oraz program szkolenia.

2.7.1. szkolenia powinny się odbyć w terminie 6 miesięcy od dnia podpisania umowy;

2.7.2. Wykonawca w ramach wykonania usługi szkoleniowej przygotuje harmonogram i program szkolenia i dostarczy go akceptacji Zamawiającego w terminie do czternastu dni od daty zawarcia umowy.

2.8. Materiały szkoleniowe

2.8.1. każdy uczestnik szkolenia otrzyma w pierwszym dniu szkolenia dostęp do certyfikowanych materiałów szkoleniowych;

2.8.2. materiały szkoleniowe muszą obejmować cały zakres merytoryczny szkolenia;

2.8.3. materiały szkoleniowe zostaną przygotowane i sporządzone w języku polskim;

2.8.4. wszelkie koszty materiałów szkoleniowych ponosi Wykonawca.

2.9. Zakres merytoryczny szkolenia

2.9.1. Bezpieczeństwo SQL Server

- Uwierzytelnianie połączeń z SQL Server
- Autoryzowanie loginów do łączenia się z bazami danych
- Autoryzacja pomiędzy serwerami
- Częściowo zawarte bazy danych

Ćwiczenia: Bezpieczeństwo SQL Server

- Uwierzytelnianie połączeń z SQL Server
- Autoryzowanie połączeń z bazami danych
- Autoryzacja pomiędzy instancjami serwera
- Autoryzowanie połączeń z bazami danych

2.9.2. Przypisywanie ról serwera i bazy danych

- Praca z rolami serwera
- Praca z ustalonymi rolami bazy danych
- Role bazy danych zdefiniowane przez użytkownika

Ćwiczenia: Przypisywanie ról serwera i bazy danych

- Korzystanie z ról serwera
- Korzystanie z ról bazy danych
- Używanie zdefiniowanych przez użytkownika ról bazy danych i ról aplikacji

2.9.3. Autoryzowanie użytkowników do dostępu do zasobów
- Autoryzowanie użytkowników do dostępu do obiektów
- Autoryzowanie użytkowników do wykonywania kodu
- Konfiguracja uprawnień na poziomie schematu

Ćwiczenia: Autoryzowanie użytkowników do dostępu do zasobów
- Przypisywanie stałych i zdefiniowanych przez użytkownika ról serwera
- Zarządzanie rolami i użytkownikami bazy danych
- Konfiguracja uprawnień na poziomie schematu

2.9.4. Ochrona danych za pomocą szyfrowania i audytu
- Opcje w zakresie audytowania dostępu do danych w SQL Server
- Wdrażanie narzędzia SQL Server Audit
- Zarządzanie narzędziem SQL Server Audit
- Ochrona danych za pomocą szyfrowania

Ćwiczenia: Stosowanie narzędzi audytu i szyfrowania
- Audyt z wykorzystaniem tabel czasowych
- Wykorzystanie SQL Server Audit
- Wyświetlanie wyników audytu
- Korzystanie z dynamicznego maskowania danych

2.9.5. Modele odzyskiwania danych i strategie tworzenia kopii zapasowych
- Zapoznanie ze strategiami tworzenia kopii zapasowych
- Dzienniki transakcji serwera SQL
- Planowanie strategii tworzenia kopii zapasowych

Ćwiczenia: Zapoznanie z modelami odzyskiwania danych SQL Server
- Kopie zapasowe baz danych
- Kopie zapasowe dzienników transakcji
- Zmniejszanie bazy danych

2.9.6. Tworzenie kopii zapasowych baz danych SQL Server
- Tworzenie kopii zapasowych baz danych i dzienników transakcji
- Zarządzanie kopiami zapasowymi baz danych
- Zaawansowane opcje baz danych

Ćwiczenia: Tworzenie kopii zapasowych baz danych
- Tworzenie kopii zapasowych baz danych
- Weryfikacja kopii zapasowych
- Korzystanie z zaawansowanych funkcji tworzenia kopii zapasowych

2.9.7. Przywracanie baz danych SQL Server
- Zrozumienie procesu przywracania
- Przywracanie baz danych
- Zaawansowane scenariusze przywracania
- Odzyskiwanie danych z konkretnego punktu w czasie

Ćwiczenia: Przywracanie baz danych SQL Server
- Określanie kolejności przywracania danych
- Przywracanie baz danych
- Przywracanie zaszyfrowanej kopii zapasowej
- Przywracanie do punktu w czasie

2.9.8. Automatyzacja procesu zarządzania SQL Server
- Automatyzacja procesu zarządzania SQL Server

- Praca z SQL Server Agent
- Zarządzanie zadaniami SQL Server Agent
- Zarządzanie wieloma serwerami

Ćwiczenia: Automatyzacja procesu zarządzania SQL Server

- Wykorzystanie SQL Server Agent
- Skrypty dla zadań SQL Server Agent
- Przeglądanie historii zadań
- Zarządzanie replikacją z wieloma wzorcami

2.9.9. Konfiguracja zabezpieczeń dla SQL Server Agent

- Zapoznanie z zabezpieczeniami SQL Server Agent
- Konfiguracja poświadczeń
- Konfiguracja kont serwera proxy

Ćwiczenia: Konfiguracja SQL Server Agent

- Przypisywanie kontekstu zabezpieczeń do kroków zawartych w zadaniu
- Tworzenie poświadczeń
- Tworzenie konta serwera proxy

2.9.10. Monitorowanie SQL Server za pomocą alertów i powiadomień

- Monitorowanie błędów SQL Server
- Konfiguracja poczty bazy danych
- Operatorzy, alerty i powiadomienia
- Alerty w Azure SQL Database

Ćwiczenia: Monitorowanie SQL Server za pomocą alertów i powiadomień

- Praca z dziennikami błędów aparatu bazy danych
- Konfiguracja poczty bazy danych
- Konfiguracja operatorów i alertów
- Konfiguracja alertów w Azure SQL Database (opcjonalnie)Wprowadzenie do zarządzania

2.9.11. SQL Server za pomocą PowerShell

Wprowadzenie do Windows PowerShell

- Konfiguracja SQL Server za pomocą PowerShell
- Administrowanie rozwiązaniem SQL Server i utrzymywanie go za pomocą PowerShell
- Zarządzanie bazami danych SQL Azure za pomocą PowerShell

Ćwiczenia: Wykorzystanie PowerShell do zarządzania SQL Server

- Zapoznanie z obiektami SQL Server Management Objects (SMO)
- Konfiguracja bazy danych i funkcji wystąpień za pomocą PowerShell
- Zarządzanie loginami i kopiami zapasowymi za pomocą PowerShell
- Tworzenie bazy danych Azure SQL za pomocą PowerShell

2.9.12. Śledzenie dostępu do SQL Server za pomocą funkcji zdarzeń rozszerzonych

- Zdarzenia rozszerzone - podstawowe pojęcia
- Praca z funkcją zdarzeń rozszerzonych

Ćwiczenia: Wykorzystanie zdarzeń rozszerzonych SQL Server

- Tworzenie sesji zdarzeń rozszerzonych
- Praca z sesjami zdarzeń rozszerzonych

2.9.13. Monitorowanie SQL Server

- Monitorowanie aktywności
- Przechwytywanie danych dotyczących wydajności i zarządzanie nimi

- Analiza zebranych danych dotyczących wydajności

Ćwiczenia: Monitorowanie SQL Server

- Korzystanie z monitora wydajności
- Konfiguracja gromadzenia danych
- Przeglądanie raportów

2.9.14. Rozwiązywanie problemów z narzędziem SQL Server

- Stosowanie metodologii rozwiązywania problemów
- Rozwiązywanie problemów związanych z usługami
- Rozwiązywanie problemów z połączeniem i logowaniem

Ćwiczenia: Rozwiązywanie problemów z SQL Server

- Rozwiązywanie problemów z błędami
- Rozwiązywanie problemów z usługami
- Rozwiązywanie problemów z logowaniem

2.9.15. Importowanie i eksportowanie danych

- Przesyłanie danych do i z SQL Server
- Import i eksport danych tabeli
- Używanie funkcji BCP i BULK INSERT do importu danych
- Wdrażanie aplikacji warstwy danych

Ćwiczenia: Importowanie i eksportowanie danych

- Wyłączanie i włączanie ograniczeń
- Korzystanie z kreatora importu i eksportu
- Importowanie za pomocą funkcji BCP oraz BULK INSERT
- Praca z narzędziami DACPAC oraz BACPAC

2.10. **Trener realizujący usługę szkoleniową:** musi posiadać certyfikat wystawiony przez Producenta oprogramowania Zamawiającego, to jest: certyfikat Microsoft Certified Trainer (MCT), a w przypadku zaoferowania szkolenia równoważnego: certyfikat wystawiony przez Producenta oprogramowania równoważnego, uprawniający do prowadzenia szkoleń z zakresu konfigurowania i administrowania urządzenia równoważnego.

2.11. **Certyfikat ukończenia szkolenia:** po ukończeniu szkolenia, uczestnicy szkolenia otrzymują certyfikat ukończenia szkolenia sygnowany przez Producenta oprogramowania Zamawiającego.

3. Szkolenie: Rozwiązywanie problemów i wsparcie techniczne dla Windows 11

3.1. Cel usługi szkoleniowej: po ukończeniu szkolenia, uczestnik będzie potrafił: obsługiwać i rozwiązywać problemy związane urządzeniami z systemem Windows 11 w lokalnym środowisku domeny Windows Server Active Directory. Umiejętności te obejmują zrozumienie ważnych funkcji systemu Windows 11, korzystania z nich w usłudze Active Directory oraz rozwiązywania związanych z nimi problemów.

3.2. Wymóg autoryzacji szkolenia przez Producenta rozwiązania z uwagi:

3.2.1. na charakter usługi szkoleniowej oraz jej ww. cel, oraz związaną z nią potrzebę zapewnienia pełnej użyteczności wiedzy i umiejętności nabytych przez uczestników szkolenia;

3.2.2. na to, że jakość i zakres usługi szkoleniowej oraz zdobyte dzięki uczestnictwie w szkoleniu wiedza i umiejętności będą wpływać bezpośrednio na poziom cyberbezpieczeństwa Zamawiającego.

Zamawiający zastrzega, że szkolenie/szkolenie równoważne musi być autoryzowane przez Producenta posiadanych przez Zamawiającego oprogramowania firmę: Microsoft.

3.3. Forma szkolenia: szkolenie realizowane stacjonarnie w siedzibie Zamawiającego.

3.4. Język prowadzenia szkolenia: szkolenie zostanie przeprowadzone w języku polskim.

3.5. Liczba uczestników szkolenia (liczba szkolonych osób): 3 osoby (pracownicy działu IT Zamawiającego).

3.6. Czas trwania szkolenia. Szkolenie zostanie zrealizowane w następującym wymiarze:

3.6.1. liczba dni: minimum 4 dni;

3.6.2. liczba godzin: minimum 32 godziny lekcyjnych, w tym minimum 16 godzin laboratoriów (zajęć praktycznych).

3.7. Termin szkolenia, harmonogram oraz program szkolenia.

3.7.1. szkolenia powinny się odbyć w terminie 6 miesięcy od dnia podpisania umowy;

3.7.2. Wykonawca w ramach wykonania usługi szkoleniowej przygotuje harmonogram i program szkolenia i dostarczy go do akceptacji Zamawiającego w terminie do czternastu dni od daty zawarcia umowy.

3.8. Materiały szkoleniowe

3.8.1. każdy uczestnik szkolenia otrzyma w pierwszym dniu szkolenia dostęp do certyfikowanych materiałów szkoleniowych;

3.8.2. materiały szkoleniowe muszą obejmować cały zakres merytoryczny szkolenia;

3.8.3. materiały szkoleniowe zostaną przygotowane i sporządzone w języku polskim;

3.8.4. wszelkie koszty materiałów szkoleniowych ponosi Wykonawca.

3.9. Zakres merytoryczny szkolenia

3.9.1. Wprowadzenie do Windows 11

- Przegląd systemu Windows 11
- Nowe funkcje w Windows 11
- Znaczące zmiany z Windows 10
- Zmiany w interfejsie użytkownika
- Zawiera przegląd architektury systemu, w tym podsystemów Linux i Android
- Rozwiązywanie problemów z instalacją i wdrażaniem
- Przegląd wymaganego sprzętu, identyfikowanie różnic w stosunku do systemu Windows 10
- Problemy z uaktualnieniem do systemu Windows 11
- Zalecenia dotyczące typowych procedur rozwiązywania problemów
- Wprowadzenie do narzędzi do rozwiązywania problemów
- Menadżer zadań
- Monitor zasobów
- Monitor wydajności
- Przegląd poprawionej aplikacji ustawień

3.9.2. Zdalne administrowanie systemem Windows 11

- Przegląd narzędzi administracyjnych
- Korzystanie ze zdalnego pulpitu
- Korzystanie z szybkiej pomocy
- Korzystanie z Centrum administracyjnego systemu Windows
- Wprowadzenie do Windows PowerShell
- Komunikacja zdalna za pomocą programu Windows PowerShell
- Włączanie komunikacji zdalnej PowerShell

- Zaufane hosty

3.9.3. Rozwiązywanie problemów z uruchamianiem i przywracaniem systemu
- Przegląd środowiska odzyskiwania systemu Windows 11
- Konfiguracja rejestru
- Rozwiązywanie problemów z ustawieniami uruchamiania
- Odzyskiwanie dysków chronionych funkcją BitLocker
- Rozwiązywanie problemów z usługą systemu operacyjnego
- Odzyskiwanie komputera
- Rozwiązywanie problemów z urządzeniami i sterownikami urządzeń
- Przegląd rozwiązywania problemów ze sprzętem
- Ustawienia zasad grupy, które mogą kontrolować/wstrzymywać instalację sprzętu
- Rozwiązywanie problemów z awariami sterowników urządzeń

3.9.4. Konfiguracja i rozwiązywanie problemów z łącznością sieciową
- Identyfikacja nieprawidłowo skonfigurowanej sieci i ustawień TCP/IP
- Omówienie adresowania podsieci IPv4 ułatwiające identyfikację nieprawidłowo skonfigurowanych urządzeń
- Określanie ustawień sieciowych
- Rozwiązywanie problemów z łącznością sieciową
- Rozwiązywanie problemów z rozwiązywaniem nazw
- Przegląd zdalnego dostępu
- Rozwiązywanie problemów z połączeniem VPN

3.9.5. Rozwiązywanie problemów z zasadami grupy
- Przegląd zasad grupy
- Rozwiązywanie problemów z konfiguracją klienta i aplikacjami GPO

3.9.6. Konfiguracja i rozwiązywanie problemów z ustawieniami bezpieczeństwa
- Bezpieczny, zaufany i mierzony rozruch
- Ustawienia UEFI
- Wymagania TPM
- Wdrażanie zabezpieczeń sieciowych za pomocą Zapory Windows Defender i Zapory Windows Defender z zabezpieczeniami zaawansowanymi
- Wdrażanie funkcji Credential Guard, Exploit Guard i Application Guard
- Konfiguracja Windows Hello
- Rozwiązywanie problemów z logowaniem

3.9.7. Konfiguracja i rozwiązywanie problemów ze stanem użytkownika
- Rozwiązywanie problemów z zastosowaniem ustawień użytkownika
- Konfiguracja i rozwiązywanie problemów UE-V
- Konfiguracja i rozwiązywanie problemów z przekierowaniem folderu

3.9.8. Konfigurowanie i rozwiązywanie problemów z dostępem do zasobów
- Rozwiązywanie problemów z uprawnieniami do plików
- Rozwiązywanie problemów z drukarkami
- Odzyskiwanie plików w systemie Windows 11

3.9.9. Rozwiązywanie problemów z aplikacjami
- Rozwiązywanie problemów z aplikacjami komputerowymi
- Zarządzanie uniwersalnymi aplikacjami Windows
- Przegląd kontroli aplikacji

- Rozwiązywanie problemów z aplikacją AppLocker Policy
- Rozwiązywanie problemów ze zgodnością aplikacji
- Konfiguracja trybu kiosku

3.9.10. Utrzymanie Windows 11

- Monitorowanie i rozwiązywanie problemów z wydajnością komputera
- Przegląd Windows Update
- Konfiguracja Windows Update dla firm
- Rozwiązywanie problemów z aktualizacjami systemu Windows

3.10. **Trener realizujący usługę szkoleniową:** musi posiadać certyfikat wystawiony przez Producenta oprogramowania Zamawiającego, to jest: certyfikat Microsoft Certified Trainer (MCT), a w przypadku zaoferowania szkolenia równoważnego: certyfikat wystawiony przez Producenta oprogramowania równoważnego, uprawniający do prowadzenia szkoleń z zakresu konfigurowania i administrowania urządzenia równoważnego.

3.11. **Certyfikat ukończenia szkolenia**: Po ukończeniu szkolenia, uczestnicy szkolenia otrzymują certyfikat ukończenia szkolenia sygnowany przez Producenta oprogramowania Zamawiającego.

4. Szkolenie: Konfigurowanie i administrowanie Hyper-V

4.1. Cel usługi szkoleniowej: po ukończeniu szkolenia, uczestnik będzie potrafił konfigurować oraz administrować Hyper-V w Windows Server.

4.2. Wymóg autoryzacji szkolenia przez Producenta rozwiązania z uwagi:

4.2.1. na charakter usługi szkoleniowej oraz jej ww. cel, oraz związaną z nią potrzebę zapewnienia pełnej użyteczności wiedzy i umiejętności nabytych przez uczestników szkolenia;

4.2.2. na to, że jakość i zakres usługi szkoleniowej oraz zdobyte dzięki uczestnictwie w szkoleniu wiedza i umiejętności będą wpływać bezpośrednio na poziom cyberbezpieczeństwa Zamawiającego;

Zamawiający zastrzega, że szkolenie/szkolenie równoważne musi być autoryzowane przez Producenta posiadanych przez Zamawiającego oprogramowania firmę: Microsoft.

4.3. Forma szkolenia: szkolenie realizowane stacjonarnie w siedzibie Zamawiającego.

4.4. Język prowadzenia szkolenia: szkolenie zostanie przeprowadzone w języku polskim

4.5. Liczba uczestników szkolenia (liczba szkolonych osób): 3 osoby (pracownicy działu IT Zamawiającego).

4.6. Czas trwania szkolenia. Szkolenie zostanie zrealizowane w następującym wymiarze:

4.6.1. liczba dni: minimum 3 dni;

4.6.2. liczba godzin: minimum 24 godziny lekcyjnych, w tym minimum 10 godzin laboratoriów (zajęć praktycznych).

4.7. Termin szkolenia, harmonogram oraz program szkolenia

4.7.1. szkolenia powinny się odbyć w terminie 6 miesięcy od dnia podpisania umowy;

4.7.2. Wykonawca w ramach wykonania usługi szkoleniowej przygotuje harmonogram i program szkolenia i dostarczy go do akceptacji Zamawiającego w terminie do czternastu dni od daty zawarcia umowy.

4.8. Materiały szkoleniowe

4.8.1. każdy uczestnik szkolenia otrzyma w pierwszym dniu szkolenia dostęp do certyfikowanych materiałów szkoleniowych;

4.8.2. materiały szkoleniowe muszą obejmować cały zakres merytoryczny szkolenia;

4.8.3. materiały szkoleniowe zostaną przygotowane i sporządzone w języku polskim;

4.8.4. wszelkie koszty materiałów szkoleniowych ponosi Wykonawca.

4.9. Zakres merytoryczny szkolenia

4.9.1. Planowanie wdrożenia usług wirtualizacji
- Wprowadzenie do wirtualizacji Microsoft
- Analiza zasobów infrastruktury
- Planowanie usług wirtualizacji
- Laboratoria: Analiza zasobów infrastruktury dla usług wirtualizacji

4.9.2. Wdrażanie rozwiązań wirtualizacji serwerów Hyper-V
- Implementacja Hyper-V
- Zarządzanie składnicami danych maszyn wirtualnych
- Zarządzanie wirtualnymi sieciami
- Laboratoria: Instalacja i konfiguracja Hyper-V

4.9.3. Tworzenie i konfiguracja wirtualnych dysków i maszyn
- Tworzenie i konfiguracja wirtualnych dysków
- Tworzenie i konfiguracja maszyn wirtualnych
- Zarządzanie migawkami maszyn wirtualnych
- Import maszyn wirtualnych
- Laboratoria: Tworzenie wirtualnych dysków i maszyn

4.9.4. Konfiguracja sieci w Hyper-V
- Zaawansowane funkcje wirtualnych interfejsów sieciowych
- Wirtualizacja sieci Hyper-V
- Rozszerzenia funkcji przełączników sieciowych Hyper-V
- Laboratoria: Konfiguracja wirtualnych sieci

4.9.5. Skalowanie maszyn wirtualnych
- Wprowadzenie do opcji skalowania maszyn wirtualnych w Windows Server 2012
- Non-uniform memory access (NUMA)
- Porównanie opcji skalowania Hyper-V
- Laboratoria: Konfiguracja NUMA

4.9.6. Hyper-V Replica oraz odzyskiwanie po awarii
- Wprowadzenie do funkcji Hyper-V Replica
- Konfiguracja Hyper-V Replica
- Operacje przełączania maszyn po awarii w Hyper-V Replica
- Kopie zapasowe Hyper-V
- Laboratoria: Konfiguracja funkcji Hyper-V Replica oraz kopi zapasowych

4.9.7. Mechanizmy migracji maszyn wirtualnych w Hyper-V
- Wprowadzenie do mechanizmów Live Migration
- Wprowadzenie do mechanizmów migracji składnic danych
- Bezpieczeństwo Live Migration
- Wykorzystanie protokołu SMB w Live Migration
- Laboratoria: Wdrażanie mechanizmów migracji maszyn wirtualnych w Hyper-V

4.10. **Trener realizujący usługę szkoleniową**: musi posiadać certyfikat wystawiony przez Producenta oprogramowania Zamawiającego, to jest: certyfikat Microsoft Certified Trainer (MCT), a w przypadku zaoferowania szkolenia równoważnego: certyfikat wystawiony przez Producenta oprogramowania równoważnego, uprawniający do prowadzenia szkoleń z zakresu konfigurowania i administrowania urządzenia równoważnego.

4.11. **Certyfikat ukończenia szkolenia**: po ukończeniu szkolenia, uczestnicy szkolenia otrzymują certyfikat ukończenia szkolenia sygnowany przez Producenta oprogramowania Zamawiającego.

5. Szkolenie: Administrowanie systemem Windows Server

5.1. Cel usługi szkoleniowej: po ukończeniu szkolenia, uczestnik będzie potrafił konfigurować oraz administrować systemami z rodziny Windows Server m.in.:

- Korzystać z technik i narzędzi administracyjnych w systemie Windows Server,
- Wdrażać usługi zarządzania tożsamością,
- Zarządzać usługami infrastruktury sieciowej,
- Konfigurować serwery plików i pamięć masową,
- Zarządzać maszynami wirtualnymi z wykorzystaniem wirtualizacji Hyper-V i kontenerów,
- Wdrażać rozwiązania wysokiej dostępności i odzyskiwania danych po awarii,
- Stosować zabezpieczenia w celu ochrony kluczowych zasobów,
- Konfigurować usługi zdalnego pulpitu,
- Konfigurować wdrożenie infrastruktury pulpitów opartej na maszynach wirtualnych,
- Wdrażać dostęp zdalny i usługi internetowe,
- Wdrażać monitorowanie usług i wydajności oraz rozwiązywać problemy,
- Wykonywać aktualizacje i migracje związane z AD DS, oraz pamięcią masową.

5.2. Wymóg autoryzacji szkolenia przez Producenta rozwiązania z uwagi:

5.2.1. na charakter usługi szkoleniowej oraz jej ww. cel, oraz związaną z nią potrzebę zapewnienia pełnej użyteczności wiedzy i umiejętności nabytych przez uczestników szkolenia;

5.2.2. na to, że jakość i zakres usługi szkoleniowej oraz zdobyte dzięki uczestnictwie w szkoleniu wiedza i umiejętności będą wpływać bezpośrednio na poziom cyberbezpieczeństwa Zamawiającego;

Zamawiający zastrzega, że szkolenie/szkolenie równoważne musi być autoryzowane przez Producenta posiadanych przez Zamawiającego oprogramowania firmę: Microsoft.

5.3. Forma szkolenia: szkolenie realizowane stacjonarnie w siedzibie Zamawiającego.

5.4. Język prowadzenia szkolenia: szkolenie zostanie przeprowadzone w języku polskim.

5.5. Liczba uczestników szkolenia (liczba szkolonych osób): 3 osoby (pracownicy działu IT Zamawiającego).

5.6. Czas trwania szkolenia. Szkolenie zostanie zrealizowane w następującym wymiarze:

5.6.1. liczba dni: minimum 5 dni;

5.6.2. liczba godzin: minimum 40 godziny lekcyjnych, w tym minimum 15 godzin laboratoriów (zajęć praktycznych).

5.7. Termin szkolenia, harmonogram oraz program szkolenia.

5.7.1. szkolenia powinno się odbyć w terminie 6 miesięcy od dnia podpisania umowy;

5.7.2. Wykonawca w ramach wykonania usługi szkoleniowej przygotuje harmonogram i program szkolenia i dostarczy go do akceptacji Zamawiającego w terminie do czternastu dni od daty zawarcia umowy.

5.8. Materiały szkoleniowe

5.8.1. każdy uczestnik szkolenia otrzyma w pierwszym dniu szkolenia dostęp do certyfikowanych materiałów szkoleniowych;

5.8.2. materiały szkoleniowe muszą obejmować cały zakres merytoryczny szkolenia;

5.8.3. materiały szkoleniowe zostaną przygotowane i sporządzone w języku polskim;

5.8.4. wszelkie koszty materiałów szkoleniowych ponosi Wykonawca.

5.9. Zakres merytoryczny szkolenia

5.9.1. Wprowadzenie do administracji systemu Windows Server

- Wprowadzenie do systemu Windows Server
- Wprowadzenie do systemu Windows Server Core
- Wprowadzenie do zasad i narzędzi administracyjnych systemu Windows Server

Ćwiczenie: Wdrażanie i konfiguracja systemu Windows Server

- Wdrażanie i konfiguracja systemu Server Core
- Wdrażanie i stosowanie zdalnej administracji serwerami

5.9.2. Usługi zarządzania tożsamością w systemie Windows Server

- Wprowadzenie do AD DS
- Wdrażanie kontrolerów domeny Windows Server
- Wprowadzenie do usługi Azure AD
- Wdrażanie zasad grupy
- Wprowadzenie do usług certyfikatów Active Directory

Ćwiczenie: Wdrażanie usług zarządzania tożsamością i zasad grupy

- Wdrażanie nowego kontrolera domeny w systemie Server Core
- Konfigurowanie zasad grupy
- Wdrażanie i korzystanie z usług certyfikatów
- Wyjaśnienie podstaw zasad grupy i konfiguracja GPO w środowisku domenowym
- Opis roli usług certyfikatów Active Directory i korzystanie z certyfikatów

5.9.3. Usługi infrastruktury sieciowej w systemie Windows Server

- Wdrażanie i zarządzanie protokołem DHCP
- Wdrażanie i zarządzanie systemem DNS
- Wdrażanie i zarządzanie systemem IPAM
- Usługi dostępu zdalnego w systemie Windows Server

Ćwiczenie: Wdrażanie i konfiguracja usług infrastruktury sieciowej w systemie Windows Server

- Wdrażanie i konfiguracja protokołu DHCP
- Wdrażanie i konfiguracja systemu DNS
- Wdrażanie serwera proxy aplikacji sieci WWW

5.9.4. Serwery plików i zarządzanie pamięcią masową w systemie Windows Server

- Woluminy i systemy plików w systemie Windows Server
- Wdrażanie udostępniania w systemie Windows Server
- Wdrażanie rozwiązania Storage Spaces (przestrzeni dyskowych) w systemie Windows Server
- Wdrażanie deduplikacji danych
- Wdrażanie interfejsu iSCSI
- Wdrażanie rozproszonego systemu plików

Ćwiczenie: Wdrażanie rozwiązań pamięci masowej w systemie Windows Server

- Wdrażanie deduplikacji danych
- Konfiguracja magazynu iSCSI
- Konfiguracja nadmiarowych przestrzeni dyskowych
- Wdrażanie Storage Spaces Direct

5.9.5. Wirtualizacja Hyper-V i kontenery w systemie Windows Server

- Hyper-V w systemie Windows Server

- Konfiguracja maszyn wirtualnych /li>
- Zabezpieczanie wirtualizacji w systemie Windows Server
- Kontenery w systemie Windows Server
- Wprowadzenie do platformy Kubernetes

Ćwiczenie: Wdrażanie i konfiguracja wirtualizacji w systemie Windows Server

- Tworzenie i konfigurowanie maszyn wirtualnych
- Instalacja i konfiguracja kontenerów

5.9.6. Wysoka dostępność w systemie Windows Server

- Planowanie wdrożenia klastra pracy awaryjnej
- Tworzenie i konfiguracja klastra pracy awaryjnej
- Wprowadzenie do rozciągniętych klastrów
- Planowanie rozwiązań w zakresie wysokiej dostępności i odzyskiwania danych po awarii z wykorzystaniem maszyn wirtualnych funkcji Hyper-V

Ćwiczenie: Wdrażanie klastra pracy awaryjnej

- Konfiguracja pamięci masowej i tworzenie klastra
- Wdrażanie i konfiguracja serwera plików o wysokiej dostępności
- Sprawdzanie poprawności wdrożenia serwera plików o wysokiej dostępności

5.9.7. Odzyskiwanie danych po awarii w systemie Windows Server

- Funkcja Hyper-V Replica
- Tworzenie kopii zapasowych i przywracanie infrastruktury w systemie Windows Server

Ćwiczenie: Wdrażanie funkcji Hyper-V Replica i Windows Server Backup

- Wdrażanie funkcji Hyper-V Replica
- Wdrażanie tworzenia kopii zapasowych i przywracania za pomocą narzędzia Windows Server Backup

5.9.8. Bezpieczeństwo systemu Windows Server

- Ochrona danych uwierzytelniających i dostępu uprzywilejowanego
- Hardening systemu Windows Server
- JEA w systemie Windows Server
- Zabezpieczanie i analiza ruchu w SMB
- Zarządzanie aktualizacjami w systemie Windows Server

Ćwiczenie: Konfiguracja zabezpieczeń w systemie Windows Server

- Konfiguracja funkcji Windows Defender Credential Guard
- Lokalizowanie problematycznych kont
- Wdrażanie rozwiązania LAPS

5.9.9. RDS (usługi pulpitu zdalnego) w systemie Windows Server

- Wprowadzenie do RDS
- Konfiguracja wdrażania pulpitu opartego na sesji
- Wprowadzenie do osobistych i połączonych pulpitów wirtualnych

Ćwiczenie: Wdrażanie RDS w systemie Windows Server

- Wdrażanie RDS
- Konfigurowanie ustawień kolekcji sesji i wykorzystywanie RDC
- Konfiguracja szablonu pulpitu wirtualnego

5.9.10. Dostęp zdalny i usługi internetowe w systemie Windows Server

- Wdrażanie sieci VPN
- Wdrażanie usługi Always On VPN

- Wdrażanie systemu NPS
- Wdrażanie serwera WWW w systemie Windows Server

Ćwiczenie: Wdrażanie obciążeń sieciowych

- Wdrażanie sieci VPN w systemie Windows Server
- Wdrażanie i konfiguracja serwera WWW

5.9.11. Monitorowanie serwera i wydajności w systemie Windows Server

- Wprowadzenie do narzędzi do monitorowania systemu Windows Server
- Korzystanie z monitora wydajności
- Monitorowanie dzienników zdarzeń w celu rozwiązywania problemów

Ćwiczenie: Monitorowanie i rozwiązywanie problemów z systemem Windows Server

- Ustanowienie bazowego poziomu wydajności
- Identyfikacja źródła problemu z wydajnością

5.9.12. Aktualizacja i migracja w systemie Windows Server

- Migracja AD DS
- Usługa migracji pamięci masowej
- Narzędzia do migracji systemu Windows Server

Ćwiczenie: Migracja obciążeń serwera

- Wdrażanie usługi migracji pamięci masowej

5.10. **Trener realizujący usługę szkoleniową:** musi posiadać certyfikat wystawiony przez Producenta oprogramowania Zamawiającego, to jest: certyfikat Microsoft Certified Trainer (MCT), a w przypadku zaoferowania szkolenia równoważnego: certyfikat wystawiony przez Producenta oprogramowania równoważnego, uprawniający do prowadzenia szkoleń z zakresu konfigurowania i administrowania urządzenia równoważnego.

5.11. **Certyfikat ukończenia szkolenia:** Po ukończeniu szkolenia, uczestnicy szkolenia otrzymują certyfikat ukończenia szkolenia sygnowany przez Producenta oprogramowania Zamawiającego.

III.2. Wymagania szczegółowe w zakresie Części 2

Część 2 obejmuje pakiet szkoleń podstawowych, budujących świadomość cyberzagrożeń i sposobów ochrony dla 112 pracowników Starostwa Powiatowego w Zduńskiej Woli i Powiatowego Centrum Pomocy Rodzinie w Zduńskiej Woli, którą należy zrealizować zgodnie z następującymi założeniami:

1. **Cel usługi szkoleniowej**: właściwe korzystanie z narzędzi informatycznych oraz podniesienie świadomości cyberzagrożeń, z uwzględnieniem skutków naruszeń zasad bezpieczeństwa informacji.
2. **Czas trwania szkolenia**: 12 godzin dydaktycznych (każda godzina dydaktyczna ma trwać minimum 45 minut) realizowanych w ciągu dwóch dni szkoleniowych, po 6 godzin dziennie w godzinach pomiędzy 8:00 a 15:00, w dni robocze.
3. **Termin szkolenia, harmonogram oraz program szkolenia**.
   3.1.1. szkolenia powinny się odbyć w terminie 6 miesięcy od dnia podpisania umowy;
   3.1.2. Wykonawca w ramach wykonania usługi szkoleniowej przygotuje harmonogram oraz program szkolenia i dostarczy go do akceptacji Zamawiającego w terminie do czternastu dni od daty zawarcia umowy.
4. **Tryb i miejsce szkolenia:** stacjonarny w Starostwie Powiatowym w Zduńskiej Woli przy ul. Złotnickiego 25 (sala konferencyjna).
5. **Liczba uczestników szkolenia**: 112 pracowników Starostwa Powiatowego w Zduńskiej Woli oraz Powiatowego Centrum Pomocy Rodzinie w Zduńskiej Woli, podzielonych na osiem grup szkoleniowych, po maksymalnie 15 osób w jednej grupie.
6. **Trener skierowany do realizacji szkolenia**: trener skierowany do prowadzenia szkolenia powinien posiadać stosowną kompetencje w przygotowaniu i przeprowadzeniu szkoleń budujących i wzmacniających świadomość cyberzagrożeń.
7. **Przerwy kawowe**: podczas każdego dnia szkoleniowego Wykonawca zapewni przerwy kawowe ciągłe, zawierające minimum: kawa, herbata (czarna, zielona, owocowa) - bez limitu; dodatki - cukier, mleko, cytryna; woda niegazowana i gazowana - bez limitu, kruche ciasteczka - 30 dag/os; mini drożdżówki - 2 szt./os; tartinki w różnych smakach - 4 szt./os.
8. **Forma szkolenia**
   8.1. wykład oraz interaktywne ćwiczenia z wykorzystaniem multimedialnych technik wirtualnych, w tym automatycznych symulacji phishinowej. Szkolenie musi być powiązane z testami socjotechnicznymi, aby zwiększyć efektywność reagowania uczestników na incydenty. Zajęcia muszą kłaść duży nacisk na umiejętności praktyczne uczestników i właściwe postępowanie w razie incydentu,
   8.2. szkolenie powinno być prowadzone w sposób przystępny i angażujący, z wykorzystaniem różnorodnych metod, takich jak prezentacje, ćwiczenia praktyczne i symulacje (w tym symulacje phishingowe, wykrywanie sytuacji zagrożenia w trakcie korzystania z serwisów społecznościowych), które mają praktycznie pokazać, jak działają ataki cybernetyczne.
9. **Wymóg symulacji ataku phishingowego**: Zamawiający wymaga przeprowadzenia symulacji ataku phishingowego na podane adresy mailowe uczestników szkolenia w liczbie: 1 przed terminem szkoleniem, 1 po terminie szkolenia. Wykonawca przedstawi raport z symulacji przeprowadzonej przed terminem szkolenia podczas trwania szkolenia prezentując dane statystyczne i omawiając zastosowaną technikę.
10. **Wymóg zapewnienia sprzętu**: Wykonawca powinien zapewnić min. 1 komputer na dwóch uczestników szkolenia.
11. **Certyfikat ukończenia i dokumentacja szkolenia**

11.1. szkolenie powinno się zakończyć testem oraz wydaniem imiennego certyfikatu dla uczestników;

11.2. Wykonawca musi prowadzić dokumentację szkoleniową, na którą składają się: lista obecności uczestników szkolenia (dzienne, oddzielne dla każdej grupy szkoleniowej) oraz lista odbioru zaświadczeń o ukończeniu szkolenia.

12. Materiały szkoleniowe

12.1. każdy uczestnik powinien otrzymać materiały szkoleniowe w formie drukowanej,

12.2. materiały szkoleniowe muszą obejmować cały zakres merytoryczny szkolenia,

12.3. materiały szkoleniowe zostaną przygotowane i sporządzone w języku polskim,

12.4. każdy uczestnik szkolenia otrzyma notes oraz długopis,

12.5. wszelkie koszty materiałów szkoleniowych ponosi Wykonawca.

13. Zakres merytoryczny szkolenia:

13.1. Wprowadzenie do Security Awareness

13.1.1. czym jest bezpieczeństwo informacji? - główne obszary budowania świadomości cyberzagrożeń (w tym: internet, social media, poczta elektroniczna, hasła, płatności elektroniczne, sprzęt mobilny),

13.1.2. aktualne trendy związane z cyberbezpieczeństwem,

13.1.3. co kieruje cyberprzestępcami? - motywy osób atakujących,

13.1.4. dlaczego można stać się ofiarą cyberataku? – stany emocjonalne wykorzystywane przez cyberprzestępców,

13.1.5. przegląd metod pozyskiwania informacji - socjotechnik wykorzystywanych przez cyberprzestępców.

13.1.6. Aspekty prawne związane z bezpieczeństwem informacji

13.2. Zagrożenia związane z korzystaniem z Internetu

13.2.1. czym jest ransomware?

13.2.2. czym charakteryzują się fałszywe bramki płatności? – jak je rozpoznawać?

13.2.3. sposoby reagowania na wyciek swoich osobistych danych,

13.2.4. fake news i dezinformacja – jak ją rozpoznawać?

13.3. Polityka haseł

13.3.1. jak powinno się budować dobre hasła? – stopień skomplikowania czy liczba znaków?

13.3.2. czym jest uwierzytelnianie dwuskładnikowe (2FA)

13.3.3. Metody przechowywania haseł

13.4. Social Media

13.4.1. przegląd możliwych zagrożeń związanych z rodzajem danych publikowanych w osobistych profilach,

13.4.2. sposoby reagowania na przejęcie konta,

13.4.3. co najlepiej zabezpiecza osobiste profile w social mediach? Jak dbać o ich bezpieczeństwo?

13.5. Strony www

13.5.1. definicje: domeny, subdomeny,

13.5.2. co to jest Typosquatting i dlaczego jest niebezpieczny?

13.5.3. cechy linku wiarygodnego – jak sprawdzać wiarygodność linku?

13.6. Phishing

13.6.1. definicja i odmiany phishing'u – jak go rozpoznać i jak się przed nim chronić?

13.7. Płatności w Internecie

13.7.1. metody płatności w Internecie – wygoda czy zagrożenie?
13.7.2. chargeback – co to jest i jak działa?
13.8. Bezpieczeństwo urządzeń mobilnych
13.8.1. jak cyberprzestępcy kradną dane przez telefon?
13.8.2. jak zapewnić bezpieczeństwo telefonu?
13.8.3. najlepszy sposób postępowania po utracie telefonu.
13.9. Jak zapewnić bezpieczeństwo danych podczas pracy zdalnej?
13.10. Bezpieczeństwo fizyczne pomieszczeń, dokumentacji, sprzętu IT, w tym zasada „czystego biurka”.

Kod CPV
79632000-3 – Szkolenie pracowników
80500000-9 – Usługi szkoleniowe
80533100-0 – Usługi szkolenia komputerowego