



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Załącznik nr 1c

Wdrożenie rozwiązań informatycznych w celu poprawienia cyberbezpieczeństwa w Urzędzie Gminy Kolno

Opis przedmiotu zamówienia

Szkolenia z zakresu cyberbezpieczeństwa.

Wykonawca zobowiązany jest do realizacji przedmiotu zamówienia zgodnie z Wytocznymi realizacji projektu „Cyberbezpieczny Samorząd” wydanymi przez NASK – Państwowy Instytut Badawczy.

Szkolenie z cyberbezpieczeństwa dla pracowników urzędu

1. Cel szkolenia:

Celem szkolenia jest podniesienie świadomości pracowników urzędu w zakresie współczesnych zagrożeń cyberbezpieczeństwa, w szczególności ataków ukierunkowanych na człowieka (socjotechnika). Uczestnicy nauczą się rozpoznawać i właściwie reagować na próby wyłudzenia informacji, stosować dobre praktyki (m.in. hasła, aktualizacje, kopie zapasowe, bezpieczne korzystanie z przeglądarki), a także poznają podstawowe aspekty prawne związane z odpowiedzialnością za naruszenia. Szkolenie obejmuje również zasady bezpiecznej pracy zdalnej i korzystania z urządzeń mobilnych oraz z firmowych zasobów (w tym przez VPN).

2. Zakres szkolenia:

Szkolenie musi obejmować co najmniej następujące obszary tematyczne:

1. Socjotechnika:

- Ataki socjotechniczne (techniki manipulacji wykorzystywane przez cyberprzestępców)
- Sposoby -w jaki sposób wyłudza się informacje?
- Wykrywanie - jak rozpoznać, że jest się celem ataku socjotechnicznego?
- Reakcja - jak prawidłowo reagować na ataki socjotechniczne?
- Jak i skąd atakujący zbierają dane na twój temat?
- Miejsca, w których zostawiamy swoje dane świadomie i nieświadomie
- Podniesienie świadomości w zakresie udostępniania informacji w Sieci

2. Dobre praktyki związane z cyberbezpieczeństwem:

- Polityka haseł – jakie hasło jest bezpieczne, jak nimi zarządzać?
- Zagadnienie aktualnego oprogramowania i kopii zapasowych
- Bezpieczna praca z przeglądarką internetową

3. Aspekty prawne:

- Odpowiedzialność pracownika przed pracodawcą za ujawnienie informacji
- Nieautoryzowane użycie systemów komputerowych
- Najczęstsze rodzaje naruszeń

4. Najpopularniejsze rodzaje ataków:

- Przegląd aktualnych ataków komputerowych wykorzystywanych przez przestępców
- Ataki przez pocztę e-mail (fałszywe e-maile)
- Ataki przez strony WWW (jak nie dać się zainfekować)
- Ataki przez komunikatory
- Ataki przez telefon (fałszywe SMS-y, przekierowania rozmów, itp.)
- Ataki APT, phishing, smishing, spearphishing, pharming, spoofing, spam, spim, scam ;
- Najczęstsze zaniedbania związane z wykorzystywaniem sprzętu komputerowego ;

5. Praca zdalna:

- Bezpieczne korzystanie z urządzeń mobilnych w podróży (telefony, tablety, laptopy)
- Bezpieczeństwo Twojego otoczenia
- Bezpieczeństwo telepracy na prywatnym komputerze
- Bezpieczny zdalny dostęp do firmowych zasobów (VPN).

3. Grupa docelowa:

Grupą docelową szkolenia są pracownicy urzędu (administracyjni i merytoryczni), którzy w swojej codziennej pracy korzystają z komputera, poczty elektronicznej, Internetu i/lub pracy zdalnej, a przez to mogą stać się celem ataków socjotechnicznych i innych zagrożeń cyberbezpieczeństwa.

4. Forma szkolenia:

- **Dopuszczalna forma szkolenia:** Stacjonarne w pomieszczeniu udostępnionym w siedzibie Zamawiającego.
- **Czas trwania:** 2,5-3 h lekcyjne na grupę - **szkolenie przewidziane dla dwóch grup** po 10-15 osób w grupie

5. Certyfikacja:

Każdy uczestnik, który ukończy szkolenie, otrzyma zaświadczenie ukończenia szkolenia.

Szkolenie dla Administratorów IT - Microsoft Windows Server Administration

1. Cel szkolenia:

Celem szkolenia jest podniesienie świadomości pracowników urzędu w zakresie współczesnych zagrożeń cyberbezpieczeństwa, w szczególności ataków ukierunkowanych na człowieka (socjotechnika). Uczestnicy nauczą się rozpoznawać i właściwie reagować na próby wyłudzenia informacji, stosować dobre praktyki (m.in. hasła, aktualizacje, kopie zapasowe, bezpieczne korzystanie z przeglądarki), a także poznają podstawowe aspekty prawne związane z odpowiedzialnością za naruszenia. Szkolenie obejmuje również zasady bezpiecznej pracy zdalnej i korzystania z urządzeń mobilnych oraz z firmowych zasobów (w tym przez VPN).

2. Zakres szkolenia:

Szkolenie musi obejmować następujące obszary tematyczne:

1. Instalacja i konfiguracja kontrolerów domeny usług AD DS

- 1.1. Omówienie usług Active Directory Domain Services (AD DS)
- 1.2. Omówienie kontrolerów domeny w środowisku AD DS
- 1.3. Wdrażanie kontrolera domeny
- 1.4. Konfiguracja i wykorzystanie Encrypted DNS (szyfrowana usługa rozpoznawania nazw) w systemie Windows Server

2. Zarządzanie obiektami w usługach AD DS

- 2.1. Zarządzanie kontami użytkowników
- 2.2. Zarządzanie grupami w usługach AD DS
- 2.3. Zarządzanie obiektami typu komputer w AD DS
- 2.4. Projektowanie, wdrażanie i zarządzanie jednostkami organizacyjnymi

3. Zarządzanie zaawansowaną infrastrukturą AD DS

- 3.1. Wprowadzenie do zaawansowanych scenariuszy wdrożeń AD DS
- 3.2. Wdrożenie rozproszonego środowiska AD DS
- 3.3. Konfiguracja i zarządzanie relacjami zaufania AD DS

4. Wdrażanie i zarządzanie lokacjami oraz replikacją AD DS

- 4.1. Omówienie mechanizmów replikacji usług AD DS
- 4.2. Projektowanie i konfigurowanie lokacji AD DS
- 4.3. Konfigurowanie i monitorowanie replikacji AD DS

5. Wdrażanie zasad grupy (Group Policy)

- 5.1. Wprowadzenie do zasad grupy i ich roli w zarządzaniu środowiskiem domenowym
- 5.2. Wdrażanie i zarządzanie obiektami zasad grupy (Group Policy Object – GPO)

5.3. Konfiguracja zakresu i przetwarzania GPO

5.4. Rozwiązywanie problemów związanych z działaniem zasad grupy

6. Zarządzanie ustawieniami użytkowników za pomocą zasad grupy

6.1. Wdrażanie szablonów administracyjnych (Administrative Templates)

6.2. Konfiguracja przekierowania folderów, instalacji oprogramowania oraz skryptów logowania/wylogowania

6.3. Konfiguracja preferencji zasad grupowych dla stacji roboczych i profili użytkowników

3. Grupa docelowa:

Grupą docelową szkolenia są pracownicy urzędu (administracyjni i merytoryczni), którzy w swojej codziennej pracy korzystają z komputera, poczty elektronicznej, Internetu i/lub pracy zdalnej, a przez to mogą stać się celem ataków socjotechnicznych i innych zagrożeń cyberbezpieczeństwa.

4. Forma szkolenia:

- **Dopuszczalna forma szkolenia:** Online (Virtual Classroom).
- **Czas trwania:** Szkolenie powinno trwać minimum 16 godzin i zostać zrealizowane w ciągu max. 3 dni roboczych

5. Certyfikacja:

Każdy uczestnik, który ukończy szkolenie, otrzyma certyfikat ukończenia autoryzowanego szkolenia Microsoft.

6. Prowadzący:

Szkolenie będzie prowadzone przez autoryzowanego trenera Microsoft z wieloletnim doświadczeniem w prowadzeniu szkoleń z zakresu administracji systemami Windows Server.

Wykonawca spełnia powyższy warunek, jeżeli wykaże, że trener prowadzący szkolenie posiada aktualny status Microsoft Certified Trainer (MCT), potwierdzony transkrypcją lub innym oficjalnym dokumentem wydanym przez Microsoft.

7. Wymagania techniczne:

Wykonawca udostępni na czas trwania szkolenia odpowiednie oprogramowanie niezbędne do wykonywania ćwiczeń praktycznych podczas szkolenia.

8. Wymagania dotyczące wykonawcy:

Wykonawca powinien posiadać minimum 10 letnie doświadczenie w sprzedaży i oferowaniu szkoleń z zakresu cyberbezpieczeństwa;

- Centrum szkoleniowe posiada Wpis do Instytucji Szkoleniowych,
- Centrum szkoleniowe gwarantuje wysoką jakość usług szkoleniowych w związku z posiadaniem certyfikatu systemu zarządzania jakością zgodnego z normą PN-EN ISO 9001:2015-10.