



Cyberbezpieczny Samorząd

Załącznik nr 2 do Zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Szkolenie pracowników i kierownictwa Urzędu Miejskiego w Oławie w zakresie cyberbezpieczeństwa

Wymagania:

- Liczba uczestników: około 100
- Grupy: minimum 3 grupy w tym jedna dedykowana dla kierownictwa urzędu
- Czas trwania: minimum 3 godziny na grupę, 2 dni robocze
- Certyfikat potwierdzający uczestnictwo
- Forma: stacjonarna – zmagający udostępni salę, projektor multimedialny i dostęp do Internetu – wykonawca dostarczy laptopa i wszystkie niezbędne materiały

Zakres:

Ataki “na człowieka” tzw. SOCJOTECHNIKA (obecnie wykorzystywane techniki manipulacji)

- Ataki socjotechniczne (techniki manipulacji wykorzystywane przez cyberprzestępców)
- Sposoby - pod jakimi pretekstami wyłudza się służbowe dokumenty?
- 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

Atak “na komputery” (demonstracje wraz z objaśnieniem metod ochrony)

- 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 oraz media społecznościowe
- Ataki przez telefon (fałszywe SMS-y, przekierowania rozmów, itp.)
- Ataki APT, phishing, smishing, spear-phishing, pharming, spoofing, spam, spim, scam

Dobre praktyki związane z bezpiecznym

- Polityka haseł – jakie hasło jest bezpieczne, jak nimi zarządzać?
- Problem aktualnego oprogramowania i kopii zapasowych



Fundusze Europejskie
na Rozwój Cyfrowy

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

- Bezpieczna praca z pakietem biurowym (Microsoft Office, Open Office)
- Bezpieczna praca z programem pocztowym (Outlook, Thunderbird, GMail)
- Bezpieczna praca z przeglądarką internetową
- Ryzyka związane ze skanowaniem/fotografowaniem dokumentów

Moduł dedykowany kierownictwu

- Bezpieczne korzystanie z urządzeń mobilnych w podróży (telefony, tablety, laptopy)
- Bezpieczne prowadzenie rozmów i negocjacji (telefonicznie i elektronicznie)
- Bezpieczne korzystanie z sieci bezprzewodowych np. w hotelach (Wi-Fi, Bluetooth)
- Bezpieczne przechowywanie i usuwanie danych (na komputerze i na pendrive)
- Bezpieczny zdalny dostęp do służbowych zasobów (VPN)
- Jak szybko i minimalnym nakładem podnieść bezpieczeństwo urzędu (w 5 krokach)

Aspekty prawne

- Odpowiedzialność pracownika przed pracodawcą za ujawnienie informacji
- Nieautoryzowane użycie systemów komputerowych
- Rażące zaniedbania związane z wykorzystywaniem sprzętu komputerowego

2. Szkolenia pracowników IT Urzędu Miejskiego w Oławie z zakresu bezpieczeństwa sieci komputerowych i systemów Windows

Szkolenie A - Szkolenie pracowników IT Urzędu Miejskiego w Oławie z zakresu bezpieczeństwa sieci komputerowych:

Wymagania:

- Liczba uczestników: 1
- Czas trwania: 3 dni
- Materiały szkoleniowe
- Szkolenie musi się odbywać na maszynie wirtualnej udostępnionej przez wykonawcę umożliwiającej wykonanie ćwiczeń praktycznych
- Certyfikat potwierdzający uczestnictwo
- Forma: On-line

Zakres:



Fundusze Europejskie
na Rozwój Cyfrowy

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

- a) Jak testować bezpieczeństwo sieci, czym są testy penetracyjne?
- Metodologia i rodzaje pentestów
 - OSSTMM / OWASP
 - Dokumenty opisujące dobre praktyki (NIST/CIS)
 - Różnice pomiędzy pentestami a audytami
- b) Organizacja testów penetracyjnych
- Prawne aspekty prowadzenia testów penetracyjnych
 - Opracowanie planu testów penetracyjnych
 - Popularne problemy spotykane podczas testów penetracyjnych
- c) Poszczególne fazy testu penetracyjnego
- Rekonesans
 - pasywne metody zbierania informacji o celu
 - - wykorzystanie serwerów proxy
 - - zbieranie metadanych (google hacking)
 - - profilowanie pracowników
 - - ataki typu social-engineering i APT
 - aktywne metody zbierania informacji o celu
 - - mapowanie sieci ofiary
 - - omijanie firewalli
 - Enumeracja podatności
 - rodzaje podatności (buffer overflow, format string, etc.)
 - - czym jest shellcode?
 - - mechanizmy DEP/ASLR i ich omijanie
 - - ROP i heap spray'ing
 - dopasowywanie exploita do znalezionych podatności
 - - rodzaje exploitów
 - - wyszukiwanie exploitów
 - - analiza przykładowego exploita
 - - tworzenie własnego exploita
 - wybór drogi wejścia do systemu
 - Atak
 - przegląd technik ataków na systemy i sieci komputerowe
 - ataki denial of service
 - fuzzing
 - atak przy pomocy exploita zdalnego
 - narzędzia wspomagające atak
 - podniesienie uprawnień do poziomu administratora
 - exploity lokalne
 - łamanie hashy haseł
 - Zacieranie śladów
 - backdoorowanie przejętego systemu
 - zacieranie śladów
 - Sporządzenie raportu z testu penetracyjnego
 - budowa szczegółowego raportu
 - raport dla zarządu
- d) Metody ochrony przed atakami





Cyberbezpieczny Samorząd

- Idea honeypotów
- Systemy IDS/IPS
- Metody hardeningu systemów operacyjnych

Szkolenie B - Szkolenie pracowników IT Urzędu Miejskiego w Oławie z zakresu bezpieczeństwa systemów Windows:

Wymagania:

- Liczba uczestników: 2
- Czas trwania: 2 dni
- Materiały szkoleniowe
- Szkolenie musi się odbywać na maszynie wirtualnej udostępnionej przez wykonawcę umożliwiającej wykonanie ćwiczeń praktycznych
- Certyfikat potwierdzający uczestnictwo
- forma: stacjonarna (w siedzibie wykonawcy w odległości nie większej niż 50km od Urzędu Miejskiego w Oławie) lub on-line – w przypadku formy stacjonarnej wykonawca zapewni wyżywienie i przerwę kawową w trakcie szkolenia

Zakres:

- Narzędzia:
 - Active Directory Domain Services
 - Group Policy Object
 - Microsoft Security Compliance Toolkit
 - Local Admin Password Solution
 - Sysinternals Suite
- Rekomendacje:
 - NIST – National Institute of Standards and Technology
 - STIG – Security Technical Implementation Guides
 - CIS Security Benchmark
- Bezpieczne środowisko pracy i Centralne zarządzanie konfiguracją:
 - Access Control List – ograniczenie dla zwykłego użytkownika do tworzenia plików tylko w profilu
 - Advanced Auditing – ustawienia audytu zdarzeń w systemie
 - Event Viewer – ustawienia, archiwizacja logów
 - Event Forwarding – centralna archiwizacja logów,
 - User Rights – uprawnienia użytkownika w systemie
 - Restricted Groups – zarządzanie przynależnością do grup lokalnych
 - Security Options – opcje bezpieczeństwa systemu
 - Local Admin Password Solution – zarządzanie wbudowanymi kontami administracyjnymi
 - Services – usługi systemowe
 - AppLocker/SRP – ograniczenie uruchamianych aplikacji tylko do autoryzowanych
 - Integrity Levels – zarządzanie uprawnieniami na obiektach systemowych
 - Firewall & IPSec – systemowa zaporą sieciową



Fundusze Europejskie
na Rozwój Cyfrowy

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA



Cyberbezpieczny Samorząd

- Preferences – specyficzne zmiany w rejestrach, np. konfiguracja Adobe Reader, Java
- Folder Redirection –
- Internet Explorer 11/Edge
- Office 2013/2016/2019/2021
- Enhanced Mitigation Experience Toolkit 5.52/ Windows Defender Exploit Guard
- Windows Defender Security Center
- BitLocker – szyfrowanie dysków
- Microsoft Security Compliance Toolkit – zbiór rekomendowanych ustawień dla produktów Microsoft
- Sysinternal Suite – pakiet przydatnych narzędzi np. AccessChk, Procmon
- System Microsoft Windows – konfiguracja środowiska,
- Sysmon
- File Screening – zarządzanie zawartością na serwerze plików
- Dynamic Access Control – nowe podejście do nadawania uprawnień

Zamawiający wymieniając w niniejszym opisie nazwy własne programów lub urządzeń wskazuje, co używane jest w Urzędzie Miejskim w Oławie i w takim dedykowanym zakresie wymaga przeszkolenia.

Zamawiający wymaga aby materiały były przygotowane w wersji elektronicznej zgodnie ze standardem dostępności cyfrowej.

Ponadto prezentacja i inne materiały muszą być oznaczone znakiem UE, barw RP i znakiem Funduszy Europejskich - zestawienie znaków w załączeniu. Lista obecności osób na szkoleniu również musi zawierać takie oznaczenie.

Opracował:
Łukasz Komarnicki



Fundusze Europejskie
na Rozwój Cyfrowy

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA