SZKOLENIE PODSTAWOWE

Narzędzia ochrony danych w organizacji

SEC/TOOLS

Czas trwania: 1 dni

Wprowadzenie do tematyki ochrony danych w organizacji oraz poznanie wybranych narzędzi służących zwiększeniu bezpieczeństwa

Cele szkolenia

- Zwiększenie świadomości związanej z ochroną danych
- Poznanie narzędzi służących ochronie przetwarzanych informacji
- Skuteczne zabezpieczanie danych przechowywanych na nośnikach oraz przesyłanych w sieci

Zalety

- Zobaczysz jak łatwo podsłuchać komunikację w sieci i podszyć się pod inną osobę
- Zrozumiesz jakimi technikami zabezpiecza się dane elektroniczne
- Dowiesz się jak prawidłowo weryfikować bezpieczeństwo połączenia ze swoim bankiem lub innym serwisem internetowym
- Zapoznasz się z ustawieniami bezpieczeństwa w przeglądarce internetowej
- Nauczysz się w praktyce jak zabezpieczać swoje dane na całej drodze od nadawcy do odbiorcy za pomocą podpisu elektronicznego oraz szyfrowania
- Utworzysz zaszyfrowany dysk
- Wykorzystasz aplikację do zabezpieczonej bezpośredniej komunikacji
- Zwiększysz bezpieczeństwo przechowywania swoich haseł stosując menadżera haseł
- Praktyka przed teorią - wszystkie szkolenia technologiczne prowadzone są w formie warsztatowej. Konieczna teoria jest wyjaśniana na przykładzie praktycznych zadań
- Konkretne umiejętności - w ramach każdego szkolenia rozwijamy praktyczne umiejętności związane z daną technologią i tematyką
- Nauka z praktykami - wszyscy trenerzy na co dzień pracują w projektach, gwarantuje to dostęp do eksperckiej wiedzy i praktycznego know-how

Dla kogo?

- Szkolenie adresowane jest do szerokiego grona odbiorców, takich jak programiści, dziennikarze, handlowcy jak i menadżerowie. Wiedza i umiejętności nabyte na szkoleniu są obecnie niezbędne dla każdej osoby, która wykorzystuje komputer w codziennej pracy, komunikacji czy rozrywce

Wymagania

- Od uczestników wymagana jest podstawowa znajomość obsługi komputera

Program

1. Dlaczego i jakimi technikami chronimy informacje
    a. Dlaczego należy chronić dane
    b. Wybrane skutki utraty kontroli nad danymi
    c. Wymagania dotyczące przetwarzania danych
    d. Pojęcie podpisu cyfrowego i szyfrowania, wykorzystywane algorytmy
    e. Ramy prawne związane z ochroną informacji
    f. Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO)
    g. Rozporządzenie w sprawie identyfikacji elektronicznej i usług zaufania (eIDAS)
2. Najważniejsze zagrożenia dla danych przechowywanych na dyskach oraz przesyłanych w sieci
    a. Ujawnienie poufnych informacji
    b. Kradzież i utrata danych
    c. Ataki socjotechniczne, podszywanie się, phishing
    d. Złośliwe oprogramowanie, malware i wirusy komputerowe
3. Praktyka i narzędzia ochrony informacji
    a. Czy wszystkie dane trzeba chronić
    b. Bezpiecznie zachowania użytkownika
    c. Programy antywirusowe, ochrona przed malware
    d. Zapewnienie bezpiecznej komunikacji
    e. Bezpieczeństwo nośników informacji
    f. Kopie bezpieczeństwa
4. Idea infrastruktury klucza publicznego (PKI)
    a. Certyfikaty klucza publicznego
    b. Działanie protokołu SSL/TLS
    c. Jak bezpiecznie korzystać z połączeń SSL/TLS
    d. Listy CRL i protokół OCSP
5. Zasady bezpiecznego tworzenia i przechowywania haseł
    a. Hasła i frazy hasłowe
    b. Przechowywanie haseł, wykorzystanie menadżera haseł na przykładzie KeePass
6. Bezpieczna poczta elektroniczna
    a. Podpis cyfrowy i szyfrowanie poczty
    b. Do czego służą tokeny i karty elektroniczne
    c. Wykorzystanie PGP/GnuPG oraz S/MIME
7. Bezpieczeństwo komunikacji bezpośredniej
    a. Bezpieczeństwo komunikacji głosowej i SMS
    b. Wykorzystanie Signal
8. Zabezpieczanie danych na nośnikach
    a. Tworzenie zaszyfrowanych dysków
    b. Aplikacja VeraCrypt
9. Bezpieczeństwo urządzeń mobilnych
    a. Szyfrowanie zawartości urządzenia

b. Ochrona przed nieuprawnionym dostępem
c. Usuwanie danych z urządzenia