

Kod szkolenia: **SEC/TOOLS**

Tytuł szkolenia: **Narzędzia ochrony danych w organizacji**

Dni: 1

Opis:

Adresaci szkolenia

Wiedza przekazana na szkoleniu jest obecnie niezbędna dla każdej osoby, która wykorzystuje komputer w codziennej pracy, komunikacji czy rozrywce. Są to zarówno programiści, dziennikarze, handlowcy czy szefowie działów.

Cel szkolenia

Uczestnicy dowiedzą się jak skutecznie chronić przetwarzane informacje i dane, zarówno te przechowywane na dyskach jak i przesyłane w sieci komputerowej.

Mocne strony szkolenia

Podczas warsztatów uczestnicy:

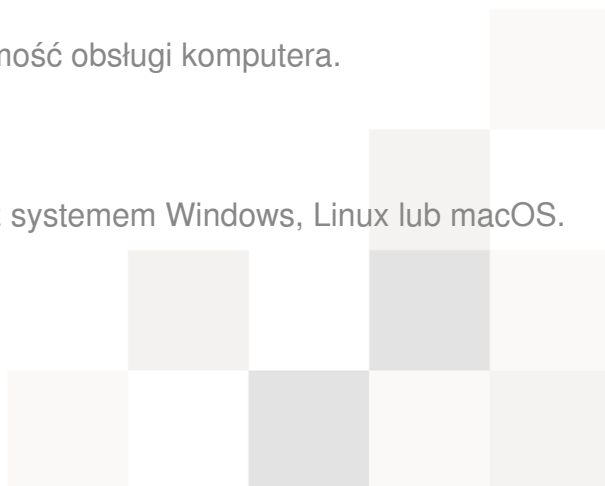
- zobaczą jak łatwo podsłuchać komunikację w sieci i podszyć się pod inną osobę,
- zrozumieją jakimi technikami zabezpiecza się dane elektroniczne,
- dowiedzą się jak prawidłowo weryfikować bezpieczeństwo połączenia ze swoim bankiem lub innym serwisem internetowym,
- zapoznają się z ustawieniami bezpieczeństwa w przeglądarce internetowej,
- nauczą się w praktyce jak zabezpieczać swoje dane na całej drodze od nadawcy do odbiorcy za pomocą podpisu elektronicznego oraz szyfrowania,
- utworzą szyfrowany dysk,
- wykorzystają aplikację do bezpiecznej bezpośredniej komunikacji,
- zwiększą bezpieczeństwo przechowywania swoich haseł stosując menadżera haseł.

Wymagania

Od uczestników wymagana jest podstawowa znajomość obsługi komputera.

Specjalne wymagania techniczne

Uczestnicy w trakcie zajęć korzystają z komputera z systemem Windows, Linux lub macOS. Niezbędne będą prawa administratora.



Parametry szkolenia

1 * 8 godzin (1 * 7 godzin netto) wykładów i warsztatów.

Program szkolenia:

1. Dlaczego i jakimi technikami chronimy informacje

- dlaczego należy chronić dane
- wybrane skutki utraty kontroli nad danymi
- wymagania dotyczące przetwarzania danych
- pojęcie podpisu cyfrowego i szyfrowania, wykorzystywane algorytmy
- ramy prawne związane z ochroną informacji
- rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO)
- rozporządzenie w sprawie identyfikacji elektronicznej i usług zaufania (eIDAS)

2. Najważniejsze zagrożenia dla danych przechowywanych na dyskach oraz przesyłanych w sieci

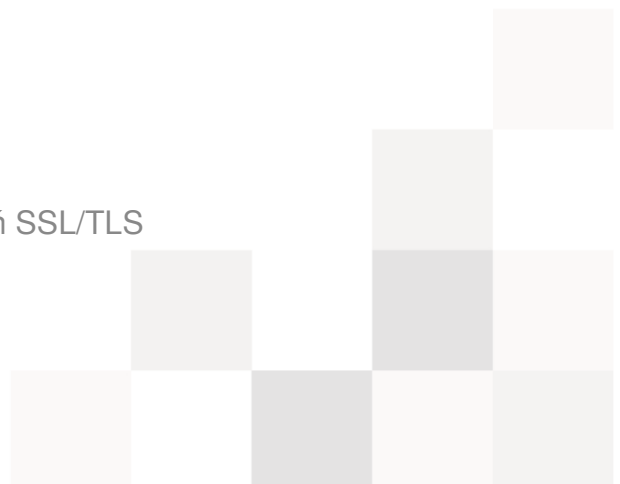
- ujawnienie poufnych informacji
- kradzież i utrata danych
- ataki socjotechniczne, podszywanie się, *phishing*
- złośliwe oprogramowanie, *malware* i wirusy komputerowe

3. Praktyka i narzędzia ochrony informacji

- czy wszystkie dane trzeba chronić
- bezpiecznie zachowania użytkownika
- programy antywirusowe, ochrona przed *malware*
- zapewnienie bezpiecznej komunikacji
- bezpieczeństwo nośników informacji
- kopie bezpieczeństwa

4. Idea infrastruktury klucza publicznego (PKI)

- certyfikaty klucza publicznego
- działanie protokołu SSL/TLS
- jak bezpiecznie korzystać z połączeń SSL/TLS
- listy CRL i protokół OCSP



5. Zasady bezpiecznego tworzenia i przechowywania haseł

- hasła i frazy hasłowe
- przechowywanie haseł, wykorzystanie KeePass

6. Bezpieczna poczta elektroniczna

- podpis cyfrowy i szyfrowanie poczty
- do czego służą tokeny i karty elektroniczne
- wykorzystanie PGP/GnuPG oraz S/MIME

7. Bezpieczeństwo komunikacji bezpośredniej

- bezpieczeństwo komunikacji głosowej i SMS
- wykorzystanie Signal

8. Zabezpieczanie danych na nośnikach

- tworzenie zaszyfrowanych dysków
- aplikacje VeraCrypt/TrueCrypt

9. Bezpieczeństwo urządzeń mobilnych

- szyfrowanie zawartości urządzenia
- ochrona przed nieuprawnionym dostępem
- usuwanie danych z urządzenia

