Szkolenie: Compendium CE
Szyfrowanie i łamanie szyfrów

FORMA SZKOLENIA	MATERIAŁY SZKOLENIOWE	CENA	CZAS TRWANIA
Stacjonarne	Tradycyjne	2400 PLN NETTO*	2 dni
Stacjonarne	Cyfrowe	2400 PLN NETTO*	2 dni
Stacjonarne	Tablet CTAB	3000 PLN NETTO*	2 dni
Metoda dlearning	Tradycyjne	2400 PLN NETTO*	2 dni
Metoda dlearning	Cyfrowe	2400 PLN NETTO*	2 dni
Metoda dlearning	Tablet CTAB	2400 PLN NETTO*	2 dni

* (+VAT zgodnie z obowiązującą stawką w dniu wystawienia faktury)

LOKALIZACJE

Kraków - ul. Tatarska 5, II piętro, godz. 9:00 - 16:00
Warszawa - ul. Bielska 17, godz. 9:00 - 16:00

DOSTĘPNE TERMINY

2019-09-11 | 2 dni | Warszawa

Cel szkolenia:

Handel elektroniczny, e-banking, podpis elektroniczny a nawet alarmy samochodowe nie mogą się obejść bez szyfrowania. Obecnie praktycznie każda przeglądarka WWW jest wyposażona w tak silne mechanizmy kryptograficzne jakimi kilkadziesiąt lat temu nie dysponowało nawet wojsko. Równocześnie co chwilę ukazują się nowe informacje o złamaniu tego czy innego szyfru, producenci prześcigają się w długościach kluczy i sile szyfrowania. Celem szkolenia ilustrowanego przykładami praktycznymi jest omówienie podstawowych zasad współczesnej kryptografii, jej silnych i słabych stron oraz możliwości ataków na systemy kryptograficzne.

Plan szkolenia:

- Cele i środki kryptografii
  - Komu jest potrzebna kryptografia?
  - Czy kryptografia to tylko szyfrowanie?
  - Szyfrowanie, kodowanie, enkrypcja, integralność, terminologia
- Historia kryptografii
  - Czasy starożytne
  - Średniowiecze

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
Alior Bank Spółka Akcyjna
Oddział w Krakowie
Nr konta: 19 2490 0005 0000 4530 5733 7313

- XIX-XX wiek
- Czasy najnowsze
- Kryptografia, polityka, terroryści

- Podstawy warsztatu kryptograficznego
  - Reguła Kerckhoffa
  - Szyfry przeszłości (Cezar, Vigenere i inne)
  - Szyfr jednorazowy (OTP)
  - Podstawowe typy ataków na szyfry
- Współczesny warsztat kryptograficzny
  - Magiczny XOR
  - Szyfry blokowe vs strumieniowe
  - Tryby pracy szyfrów blokowych
  - Funkcje skrótu i kontrola integralności
  - Szyfry symetryczne vs asymetryczne
  - Liczby losowe w kryptografii
- Szyfry blokowe
  - DES, DES-X, 3DES
  - AES
- Funkcje skrótu
  - MD5
  - SHA-1
  - SHA-2
- Szyfry asymetryczne
  - RSA
  - ElGamal
  - Krzywe eliptyczne (ECC)
- Algorytmy, protokoły
  - Algorytm a protokół
  - SSL, TLS
  - SSH
  - IPSec, ISAKMP, ESP
- Systemy kryptograficzne
  - Algorytmy, klucze, zaufanie
  - PGP
  - X.509
  - Ciphire

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
Alior Bank Spółka Akcyjna
Oddział w Krakowie
Nr konta: 19 2490 0005 0000 4530 5733 7313

- Problemy kryptografii
  - Snake-oil security
  - Security through obscurity
  - Jak rozpoznać „złą kryptografię”?

Wymagania:

Podstawowa znajomość Windows, popularnych programów pocztowych oraz biurowych.

Poziom trudności

Certyfikaty:

Uczestnicy szkolenia "**Szyfrowanie i łamanie szyfrów**" otrzymują **certyfikat** wystawiony imiennie oraz na firmę, sygnowany przez **Compendium - Centrum Edukacyjne**.

Prowadzący:

Wykładowca Compendium Centrum Edukacyjnego.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

Alior Bank Spółka Akcyjna
Oddział w Krakowie
Nr konta: 19 2490 0005 0000 4530 5733 7313