

Szkolenie: Compendium CE
Inwigilacja i szpiegostwo gospodarcze a praktyczne aspekty ochrony informacji w firmie



FORMA SZKOLENIA	MATERIAŁY SZKOLENIOWE	CENA	CZAS TRWANIA
Stacjonarne	Tradycyjne	2000 PLN NETTO*	1 dzień
Stacjonarne	Cyfrowe	2000 PLN NETTO*	1 dzień
Stacjonarne	Tablet CTAB	2600 PLN NETTO*	1 dzień

* (+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

Cel szkolenia:

Szkolenie składa się z części teoretycznej i praktycznej. Podczas trwania części praktycznej osoby biorące udział w szkoleniu mają możliwość zapoznania się z najczęściej spotykanymi urządzeniami podsłuchowymi, zasadami ich działania i instalacji, doborem kamuflażu dla urządzeń podsłuchowych oraz praktycznymi sposobami ich wykrywania przy pomocy specjalistycznych urządzeń takich jak skanery częstotliwości, analizatory widma, mierniki częstotliwości, detektory złącz nieliniowych oraz detektory kamer.

Plan szkolenia:

- o Informacja
 - o Czym jest informacja i jaką ma wartość na rynku?
 - o Potrzeby informacyjne podmiotów gospodarczych i instytucji.
 - o Źródła informacji.
- o Wywiad i kontrwywiad gospodarczy
 - o Rodzaje wywiadu oraz ich charakterystyka (biały, szary, czarny).
 - o Zadania wywiadu gospodarczego,
 - o Zainteresowania wywiadu gospodarczego.
 - o Sposoby opisu zjawisk i osób.
 - o Cykl wywiadu gospodarczego.
 - o Służby informacyjno-wywiadowcze (specyfika ich zadań i podziału kompetencji),
 - o Służby policyjno-prewencyjne.
 - o Podstawowe narzędzia pracy operacyjnej.

- Niebezpieczny styk szpiegostwa gospodarczego (komercyjnego) ze szpiegostwem międzynarodowym,
- Kontrwywiad gospodarczy,
- Rola wywiadu gospodarczego w zarządzaniu przedsiębiorstwem.
- Źródła zagrożeń
 - Zagrożenia osobowe i nieosobowe.
 - Zagrożenia zewnętrzne.
 - Zagrożenia wewnętrzne.
 - Zagrożenia ze strony pracowników.
 - Sytuacje i zdarzenia łatwe do potencjalnego wykorzystania w celach szpiegowskich.
- Podatność pracowników na werbunek do niejawnej pracy na rzecz konkurencji.
 - Klasyfikacja osobowych źródeł informacji.
 - Podstawowe metody pozyskiwania ich do współpracy.
- Atak socjotechniczny
 - Socjotechnika, jako podstawowe narzędzie pracy szpiega przy pozyskiwaniu nieuprawnionego dostępu do informacji.
 - Definicja ataku socjotechnicznego.
 - Dobór (typowanie) celu ataku.
 - Dobór czasu i miejsca ataku.
 - Etapy ataku socjotechnicznego:
 - praktyczne metody stosowane podczas ataku,
 - symptomy ataku,
 - czynniki ułatwiające atak socjotechniczny na firmę,
 - metody minimalizacji ryzyka skutecznego ataku socjotechnicznego,
 - zachowania zwiększające podatność na działanie socjotechniki,
 - minimalizacja/eliminacja skutków ataku socjotechnicznego,
 - działania prewencyjne.
- Inwigilacja fizyczna i techniczna
 - Wejście na teren obiektu celem pozyskania bezpośredniego dostępu do informacji (jawne, ciche, pod przykrywką).
 - Rozpoznanie obiektu oraz relacji interpersonalnych.
 - Instalacja urządzeń techniki inwigilacyjnej.
- Podstęp i inne urządzenia służące inwigilacji
 - Istota podstępu.
 - Procedury legalnego stosowania podstępu.
 - Podstęp nielegalny.
 - Urządzenia podsłuchowe audio.

- Urządzenia do podglądu video.
- Podstuch telefonów stacjonarnych i komórkowych.
- Inwigilacja komputerów i sieci komputerowych.
- Śledzenie pojazdów i osób przy pomocy urządzeń GPS.
- Zasady funkcjonowania profesjonalnego sprzętu podsłuchowego.
- Możliwości nowoczesnego podsłuchu.
- Sposoby zabezpieczenia pomieszczeń przed podsłuchem.
- Koszty związane z instalacją urządzeń podsłuchowych.
- Zasady instalacji urządzeń służących do inwigilacji
 - Zasady instalacji sprzętu.
 - Dobór miejsca.
 - Warunki konieczne.
- Wykrywanie urządzeń służących do inwigilacji

Wymagania:

- Podstawowa znajomość zagadnień związanych z ochroną informacji.

Poziom trudności



Certyfikaty:

Uczestnicy szkolenia otrzymują imienny certyfikat sygnowany przez Compendium Centrum Edukacyjne.

Prowadzący:

Wykładowca Compendium Centrum Edukacyjnego.

Szkolenie prowadzone jest przez byłych oficerów służb specjalnych oraz specjalistów z zakresu wykrywania urządzeń podsłuchowych.