Warszawa dn. 28.07.2022

Sekkura Sp. z o. o.

Sekkura Sp. z o.o.
ul. Erazma CIOŁKA 13/114
01-445 Warszawa
NIP: 5272708879
Nr rejestru działalności regulowanej RD-23/2017

OFERTA

sprawdzeń i zabezpieczeń antypodsłuchowych, audytów bezpieczeństwa, pozyskiwania informacji i szkoleń

Spis treści

1. Wprowadzenie

Informacja stanowi współcześnie kluczowy komponent strategiczny dla podmiotów gospodarczych prywatnych i państwowych, jest ona istotnym czynnikiem wytwórczym, coraz częściej postrzegana jest i szacowana jako zasób cenniejszy od środków ekonomicznych.

Celem działań firmy Sekkura Sp. z o.o. jest określenie silnych stron i luk w zakresie bezpieczeństwa, aby w jak największym stopniu chronić przedsiębiorstwo przed utratą tych najważniejszych dla interesów przedsiębiorstwa zasobów.

2. Bezpieczeństwo teleinformatyczne

Wykonujemy **sprawdzenia antypodsłuchowe** pomieszczeń i urządzeń (komputerów, laptopów, tabletów i smartfonów) oraz zajmujemy się **zabezpieczaniem antypodsłuchowym** pomieszczeń i urządzeń, a także specjalizujemy się w **niestandardowym zabezpieczeniu kontrwywiadowczym**.

2.1. Sprawdzanie antypodsłuchowe pomieszczeń

Proponujemy Państwu wykonanie sprawdzenia pomieszczeń oraz pojazdów pod kątem wykrycia zainstalowanych urządzeń podsłuchowych.

Sprawdzenie obejmuje:

-Sprawdzenie pasma radiowego w zakresie 100 kHz – 12 GHz;

-Sprawdzenie propagacji w zakresie podczerwieni IR;

-Sprawdzenie linii zasilających w przedziale częstotliwości 50kHz-140MHz.

-Wykrywanie złącz nieliniowych – ukrytych, nieaktywnych w momencie sprawdzania urządzeń podsłuchowych i rejestrujących - dyktafonów;

-Przeszukanie fizyczne pomieszczeń.

Metodologia sprawdzenia i stosowana aparatura

Do sprawdzenia używamy następujących przyrządów:

1. **Spectrum Rider FPH**

2. Specjalistyczny analizator widma firmy Rohde Schwarz pracujący w zakresie częstotliwości od 5 kHz do 4 GHz służącym do wykonywania pomiarów parametrów sygnałów RF oraz lokalizacji źródeł promieniowania RF.

3. Umożliwia prowadzenie ciągłej analizy aktywności emisji RF w całym zakresie częstotliwości.

4. Demoduluje sygnały RF typu AM i FM. Umożliwia rejestrowanie aktywności i poziomu mocy sygnałów RF w zaprogramowanym czasie.

5. Współpracuje z kierunkową anteną AARONIA umożliwiającą lokalizację źródeł emisji RF w sprawdzanej przestrzeni.

6.

7. Detektor ST031 M-Piranha;

1.Do wykrycia urządzeń aktywnych pracujących w zakresie częstotliwości 100 MHz – 12 GHz.

2.Do wykrycia urządzeń pracujących w zakresie bliskiej i dalekiej podczerwieni IR specjalistyczny detektor współpracujący z szerokopasmowym analizatorem ST031;

3.Sprawdzenie pod kątem obecności pasywnych uradzeń rejestrujących – dyktafonów.

4.Zestaw dodatkowych sensorów, przystawek umożliwiający sprawdzenie linii sieci energetycznej, linii telefonicznych, podatności infrastruktury budynku na podsłuch mikrofonami kontaktowymi oraz laserowymi.

8. Detektor ST 500 M-Piranha;

1.Do wykrycia urządzeń aktywnych pracujących w zakresie częstotliwości 100 MHz – 6 GHz.

2.Do wykrycia urządzeń pracujących w zakresie bliskiej i dalekiej podczerwieni IR.

3.Sprawdzenie pod kątem obecności pasywnych urządzeń rejestrujących – dyktafonów.

9. Szerokopasmowy odbiornik radiokomunikacyjny AR8200D;

Do wykrywania i odsłuchiwania wszystkich rodzajów modulacji analogowych WFM, NFM, SEM, WAM, NAM, AM, USB, LSB, CW, CTCSS i APC025;

10. **Detektor złącz nieliniowych Cayman ST-400.**

Do wykrywania złącz nieliniowych.

11. Urządzenie ST062

1.Do wykrywania transmisji GSM 900, 1800, UMTS, WiFi, Bluetooth 2,4 GHz oraz transmisji cyfrowych DECT.

12. Analizatora widma RIGOL DSA815-TG (detekcja i analiza sygnałów w paśmie 100kHz – 1,5 GHz)

13. Analizatora widma RIGOL DSA815-TG (detekcja i analiza sygnałów w paśmie 100kHz – 1,5 GHz)

14. **OPTIC-2**

Profesjonalny wykrywacz kamer ukrytych „Optic-2" przeznaczony jest do wykrywania i lokalizowania ukrytych (zakamuflowanych we wnętrzu) kamer typu „pinhole", niezależnie od ich statusu (włącz/wyłącz) i rodzaju sygnału wideo. Detektor jest zaprojektowany jako lornetka w gumowanej metalowej obudowie.

15. **ANALIZATOR ST-600.**

Wykrywacz aktywnych i pasywnych urządzeń podsłuchowych i kontroli linii przewodowych.

TRYB „CZUJNIK POLA MAGNETYCZNEGO" przeznaczony jest do wyszukiwania pracujących urządzeń podsłuchowych. Tryb realizowany jest poprzez odbieranie, przetwarzanie i wskazywanie sygnałów elektromagnetycznych wynikających z pracy urządzeń elektronicznych. Jako odbiornik wykorzystywana jest wbudowana antena magnetyczna. Zakres częstotliwości anteny (0,04 - 30 kHz) pozwala na detekcję urządzeń o ekranowanych obudowach.

TRYB „DETEKTOR LINII KABLOWYCH" jest przeznaczony do śledzenia kabli podczas wyszukiwania przewodowych urządzeń podsłuchowych. Ten tryb jest realizowany poprzez wysłanie sygnału testowego (o częstotliwości 455 kHz, modulowanego dwutonowym sygnałem o niskiej częstotliwości) do linii przewodowej i odebranie go za pomocą czujnika bezstykowego. Sygnał testowy jest generowany i dostarczany do kabla przez generator. Aby skompensować tłumienie sygnału, zapewniono regulację mocy generatora.

ST-600 może być używany w połączeniu z innymi urządzeniami detekcyjnymi serii ST:

- Wielofunkcyjnym urządzeniem wykrywającym ST-500 PIRANHA
- Analizatorem przewodów ST-301 „SPIDER"
- Detektorem złącz nieliniowych ST-402, ST-403 serii "CAYMAN".

16. Sprawdzenia fizyczne

Równolegle przeprowadzamy fizyczne oględziny sprzętu biurowego i pomieszczenia zwracając uwagę na kanały klimatyzacji, wentylacji itp.

17. <u>Uwaga</u>

Metodyka pracy, szczególnie detektorami typu PIRANHA polega na poszukiwaniu miejsca w sprawdzanym pomieszczeniu, w którym sygnał ma największą moc. Jeśli moc jest stała w całym pomieszczeniu, świadczy to o zewnętrznym źródle sygnału – nie pochodzi więc on z nadajnika urządzenia podsłuchowego. Identyfikacja źródła sygnału jest w takim wypadku nieistotna.

Po zakończeniu sprawdzenia przygotowywany jest protokół wykonanych czynności, wraz z załączonymi skanami w formie elektronicznej.

Cena:
Zależy od wielkości pomieszczeń oraz lokalizacji obiektu. Jeśli czynności mają być wykonane poza Warszawą, do ceny doliczamy koszty dojazdu oraz ewentualnego pobytu.

2.2. Zabezpieczanie pomieszczeń

Na zlecenie klienta, przygotowujemy tak zwane bezpieczne pomieszczenia, w których bezpiecznie można prowadzić rozmowy na tematy kluczowe dla interesów firmy lub instytucji. Do realizacji zlecenia stosujemy generatory szumu zabezpieczające przed podsłuchem laserowym, mikrofonami kontaktowymi i kierunkowymi. Ultradźwiękowe zagłuszarki mikrofonów. Wykładziny wygłuszające. Zakres prac jest określany podczas wizji lokalnej.

Cena.
Cena zależy od wielkości oraz zakresu niezbędnych prac i jest podawana na indywidualne pytanie klienta.

2.3. Doraźne zabezpieczanie spotkań odbywających się poza siedzibą przedsiębiorstwa

Zabezpieczenie pod względem propagacji w zakresie GSM, Bluetooth, WiFi, mikrofonami kontaktowymi i laserowymi oraz zabezpieczenie przed urządzeniami podsłuchowymi wykorzystującymi sieć elektryczną do przenoszenia sygnału.

Cena:
Zależy od wielkości pomieszczeń czasu pracy oraz lokalizacji obiektu. Jeśli czynności mają być wykonane poza Warszawą, do ceny doliczamy koszty dojazdu oraz ewentualnego pobytu.

2.4. Zabezpieczanie antypodsłuchowe urządzeń (komputerów i smartfonów)

Świadczymy usługi w zakresie wdrażania systemów bezpiecznej komunikacji w przedsiębiorstwie.

Zabezpieczenie *hi-tech* **(wysokie koszty, umiarkowana lub pomijalna niewygoda użytkowania, długi czas realizacji zamówienia i konfiguracji urządzeń, wysokie bezpieczeństwo lub nieznany stopień bezpieczeństwa[1]). Obejmuje ono zabezpieczenia programistyczne lub sprzętowe:**

- **Zabezpieczenie programistyczne.** Komercyjne oprogramowanie zapewniające szyfrowanie rozmów telefonicznych (np. Secure Voice).
- **Zabezpieczenie sprzętowe.** Antypodsłuchowe aparaty telefoniczne (np. Blackphone z PrivOS, Tripleton Enigma, XCell Basic – różnią się one funkcjonalnością i ceną).

Zabezpieczenie *low-tech* **(bardzo niskie koszty, znaczna niewygoda, szybki czas realizacji zamówienia, średnie bezpieczeństwo – potwierdzone przez środowisko ekspertów). Również obejmuje ono zabezpieczenia programistyczne i sprzętowe:**

- **Zabezpieczenia programistyczne.** Obejmują zabezpieczenia przed ingerencją fizyczną (szyfrowanie telefonu), zabezpieczenia komunikacyjne (oprogramowanie zapewniające względnie bezpiecznie korzystanie z rozmów głosowych, komunikacji tekstowej, e-mail oraz Internetu, a także monitoring telefonu i połączeń na okoliczność potencjalnego podsłuchu – wymaga zainstalowania i skonfigurowania szeregu programów jawnoźródłowych), a także przeszkolenie w zakresie technik podsłuchu pod kątem bezpiecznego

1 Jakość zabezpieczeń określa sama firma wytwarzająca i sprzedająca, brak weryfikacji przez środowisko znawców, jak w projektach typu Open Source.

używania urządzeń telekomunikacyjnych oraz przeszkolenie w zakresie właściwego użytkowania tego typu programów.

- **Zabezpieczenia sprzętowe.** Krótkotrwałe używanie tanich aparatów telefonicznych („jednorazówek") ze zanonimizowanymi kartami sim. Procedury ich pozyskiwania i zasady używania wymagają krótkiego przeszkolenia.

Cena:
Wycena indywidualna, do uzgodnienia w zależności od zapotrzebowań Klienta

3. Audyty bezpieczeństwa

Realizujemy audyty bezpieczeństwa teleinformatycznego, informacyjnego oraz fizycznego. Posiadamy unikatową, wyróżniającą nas na tle konkurencji metodykę kompleksowej ewaluacji poziomu bezpieczeństwa przedsiębiorstwa.

3.1. Audyt bezpieczeństwa teleinformatycznego urządzeń (komputerów, laptopów, tabletów, smartfonów)

Lokalny audyt bezpieczeństwa obejmuje pojedyncze komputery i inne urządzenia (tablety, laptopy, notebooki, netbooki, smartfony). Specjalizujemy się w badaniu najbardziej rozpowszechnionych systemów operacyjnych – z rodziny Windows. Celem audytu jest identyfikacja i neutralizacja zagrożeń takich jak oprogramowanie szpiegowskie czy inne złośliwe oprogramowanie (robaki, wirusy, konie trojańskie, adware, spyware, rogueware, rootkit i in.) oraz – w efekcie – podwyższenie parametrów bezpieczeństwa audytowanego systemu. Audyt obejmuje:

1. Analizę uruchomionych procesów systemu operacyjnego;
2. Weryfikację programów uruchamianych wraz z rozruchem systemu (autostart);
3. Przegląd *Harmonogramu zadań* systemu;
4. Eksplorację *Dziennika zdarzeń*;
5. Eksplorację wybranych kluczy *Edytora rejestru*;
6. Inspekcję konfiguracji przeglądarek internetowych;
7. Analizę konfiguracji sieciowej;
8. Automatyczne skanowanie pod kątem oprogramowania inwigilującego oraz luk w systemie.

Raport z przeprowadzonego audytu obejmuje wnioski i rekomendacje, a także coaching, wspólne z audytorem zwiększenie bezpieczeństwa systemu wedle przedstawionych zaleceń.

Cena:
2500 PLN za jeden komputer **1000 PLN za telefon lub tablet** **Jeśli konieczne jest przygotowanie analizy sądowej cena może wzrosnąć do 4000zł komputer/2500 zł telefon**

3.2. Audyt bezpieczeństwa sieci i witryn internetowych

Zdalny audyt bezpieczeństwa obejmuje sieci komputerowe podłączone do sieci Internet. Skupia się na dwóch komplementarnych elementach – identyfikacji i ewaluacji potencjalnych zagrożeń bezpieczeństwa powodowanych **czynnikiem teleinformatycznym**, bądź **czynnikiem ludzkim**.

W ramach aspektu teleinformatycznego oferujemy analizę topologii i funkcjonowania sieci komputerowych i serwisów www dostępnych poprzez Internet. Zakres usług obejmuje tak zwane testy penetracyjne z minimalną wiedzą (*black box*):

•**Rekonesans / gromadzenie informacji** (Google Hacking, identyfikacja subdomen, wyszukiwanie hostów wirtualnych (vhosts), ICMP Ping, Whois Lookup);

•**Testowanie aplikacji www** (URL Fuzzer - ukryte pliki i katalogi), Web Server Scan, ew. także WordPress/SharePoint/Drupal Scan);

•**Testowanie infrastruktury** (m.in. np. Ping Sweep, TCP/UDP Port Scan, DNS Zone Transfer, SSL Heartbleed Scan, SSL POODLE Scan, SSL DROWN Scan, Bash ShellShock vulnerability scanner, GHOST glibc vulnerability scanner).

Wykorzystujemy programy: m.in. Metasploit, Wireshark, W3af, BackTrack, Netsparker, Nessus, Portswigger, Social Engineering Toolkit, FOCA.

Badanie podatności czynnika ludzkiego ogniskuje się na systematycznym sprawdzaniu możliwych scenariuszy pozyskania informacji przez osoby nieuprawnione metodą inżynierii społecznej (*social engineering, phishing,* ew. *pharming*).

Cena:
Wycena indywidualna, do uzgodnienia w zależności od zapotrzebowań Klienta

3.3. Kompleksowy audyt zagrożeń przedsiębiorstwa

Cel podjętych działań analitycznych stanowi identyfikacja silnych stron i luk w zakresie bezpieczeństwa poddawanego audytowi przedsiębiorstwa i w następstwie wskazanie rekomendacji dla poszczególnych aspektów: informatycznego, technicznego, infrastrukturalnego i ludzkiego.

Zakres analizy zagrożeń

Obszar	Temat	Zadanie	Cel	Opis
Podatności na podsłuchy i inwigilację elektroniczną	Podatność na inwigilacje opartą o zastosowanie mikrofonów kierunkowych i laserowych	Ocena bezpieczeństwa pomieszczeń, w których podejmowane są decyzje żywotne dla interesów firmy pod względem możliwości zastosowania urządzeń podsłuchowych.	Ocena umiejscowienia pomieszczeń, otoczenia	Standardowa ewaluacja obejmuje: 1. Analizę pasma radiowego w zakresie 100 kHz – 14 GHz; 2. Analizę propagacji w zakresie podczerwieni IR; 3. Analizę linii zasilających w przedziale częstotliwości 50kHz-140MHz. 4. Analizę możliwości umiejscowienia ukrytych, urządzeń podsłuchowych i rejestrujących;
			Ocena możliwości wykorzystania urządzeń podsłuchowych	
	Podatność na inwigilacje wykorzystującą sieć energetyczną jako medium przenoszenia sygnałów z urządzeń podsłuchowych	Ocena bezpieczeństwa pomieszczeń, w których podejmowane są decyzje żywotne dla interesów firmy pod względem możliwości zastosowania urządzeń podsłuchowych.	Ocena zabezpieczenia sieci energetycznej.	
			Ocena możliwości wykorzystania urządzeń podsłuchowych	
	Podatność na inwigilacje wykorzystującą sieć GSM	Ocena bezpieczeństwa pomieszczeń, w których podejmowane są decyzje żywotne dla interesów firmy pod względem możliwości zastosowania urządzeń podsłuchowych.	Pomiar widma elektromagnetycznego w wybranych pomieszczeniach.	
			Ocena możliwości wykorzystania urządzeń podsłuchowych	
Scenariusze zamachów — podatność na	Analiza zagrożeń z tzw. ekip serwisowych,	Ocena możliwość wniesienia ładunków wybuchowych na teren obiektu.	Sprawdzenie możliwych scenariuszy wykonania zamachu bombowego.	Analiza procedur dostępu gości i dostawców oraz ich pojazdów do poszczególnych obszarów obiektu (w podziale na: strefę ochrony wewnętrznej, strefę ochrony obrysowej, strefę ochrony peryferyjnej/strefę

	catering, media, pogotowie gazowe, służby ratownicze			podejścia, strefę ochrony obwodowej/perymetryczną oraz strefę dozoru zewnętrznego). Analiza metodyki identyfikacji osób i pojazdów (określone procedurami *vs* realizowane). Zakres dostępu osób potencjalnie niebezpiecznych do obszarów infrastruktury krytycznej. Ocena stopnia integracji zabezpieczeń elektronicznych i mechanicznych z interwencją fizyczną. Analiza zostanie poprowadzona w czterech obszarach: systemów kontroli dostępu, systemów alarmowych oraz systemów dozorowych (monitorowania), funkcjonowania czynnika ludzkiego.
ataki wewnętrzne / sabotaż.	Wrażliwość stref oraz obszarów i obiektów.	Reakcja służb ochrony na zagrożenia	Próba wniesienia/wwiezienia materiału wybuchowego przy wykorzystaniu służb serwisowych	Przygotowanie i realizacja scenariusza ataku bombowego. Pomiar czasu opóźnienia detekcji, czasu interwencji (*versus* czas skutecznego ataku). Pomiar stopnia zgodności interwencji z istniejącymi procedurami, aktami paraprawnymi (regulaminami) i aktami prawnymi, ocena stopnia adekwatności i skuteczności reakcji personelu odpowiedzialnego za ochronę. Scenariusz zostanie przygotowany według wskazań wynikających z opracowania: *Reference Manual to Mitigate Potential Terrorist Attacks against Buildings*, US Federal Emergency Management Agency, 2003.
			Wykonanie „wrzutki"	Analiza reakcji personelu odpowiedzialnego za bezpieczeństwo oraz kierownictwa na fałszywy alarm. Scenariusz zostanie przygotowany według wskazań wynikających z opracowania: *Reference Manual to Mitigate Potential Terrorist Attacks against Buildings*, US Federal Emergency Management Agency, 2003.
	Przeprowadzenie testów tzw. penetracyjnych i sprawdzenie zachowań, przestrzeganie instrukcji oraz regulaminów	Sprawdzenie możliwości realizacji opracowanych scenariuszy.	Reakcja na próbę wtargnięcia na obiekt.	Przygotowanie i realizacja scenariusza przeniknięcia na obiekt. Pomiar czasu opóźnienia detekcji, czasu interwencji (*versus* czas skutecznego ataku). Pomiar stopnia zgodności interwencji z istniejącymi procedurami, aktami paraprawnymi (regulaminami) i aktami prawnymi, ocena stopnia adekwatności i skuteczności reakcji personelu odpowiedzialnego za ochronę.
Wskazanie słabych/mocnych stron ochrony technicznej – umiejscowienie CCTV, barier, środków ochrony technicznej,	Zabezpieczenie przed wtargnięciem obcych pojazdów na teren obiektów	Analiza możliwości sforsowania bram wjazdowych w celu dokonania zamachu.	Sprawdzenie podatności ochrony technicznej na penetrację	Analiza zostanie podjęta według wskazań doktryny *Crime Prevention Through Environmental Design* – CPETD C. Raya Jeffreya. Obejmuje ona następujące aspekty: a. kontrolę dostępu (*access control*): analiza procedur dostępu do bram wjazdowych. Zasady parkowania pojazdów i lokalizacja parkingów względem budynków. Zasady identyfikacji pojazdów pracowników/gości/dostawców i ich kierowców. Procedury i praktyczne funkcjonowanie ochrony fizycznej (strażników), mechanicznej (zamki), elektronicznej (czujniki i sygnalizatory

innych				włamania, karty dostępu i urządzenia biometryczne). b. wzmocnienie terytorialne (*territorial reinforcement*): ocena jakości zabezpieczenia stref chronionych (ogrodzenia, mury i patrole) oraz stref bezpieczeństwa uniemożliwiających atak na budynek przy użyciu bomby samochodowej. Sposób organizacji ruchu kołowego/pieszego i bariery tworzone przez elementy małej architektury: mury oporowe, kwiatony, rzeźby, ławy, maszty, słupki. Podjęcie testów weryfikujących ze szczególnym uwzględnieniem elementów socjotechnicznych.
		Sprawdzenie możliwości identyfikacji osób i pojazdów przy użyciu monitoringu.	Sprawdzenie możliwości wykrycia potencjalnych sprawców.	Identyfikacja osób i pojazdów przy użyciu monitoringu obejmuje trzy następujące aspekty: Aspekt techniczny, to jest analizę parametrów technicznych systemów monitorujących, w tym rozdzielczość rejestrowanego obrazu, głębię koloru obrazu, format i sposób przekazywania danych oraz zastosowane metody kompresji, wbudowane w kamery mechanizmy wstępnego przetwarzania danych (np. wykrywanie obiektów żywych/ruchomych w monitorowanym obszarze, identyfikacja kierunku przemieszczanie się obiektu, czujniki termowizyjne, wbudowane mechanizmy przekazywania informacji o zidentyfikowanym poruszającym się obiekcie – do innych kamer, w zależności od kierunku poruszania się). Aspekt proksemiczny systemu monitoringu wizyjnego, czyli określenie rodzaju, liczby kamer i ich rozmieszczenia, a także usytuowania i warunków pracy punktów doglądu. Pozwoli to na stworzenie „mapy pokrycia" obserwowanego terenu, a w szczególności wskazania martwych stref, określenie możliwości obserwacji wnętrz i terenu wokół obiektu, szczególnie punktów kluczowych: dojść i wejść, Aspekt organizacyjny – obejmujący analizę procedur zarządzania informacją pozyskiwaną w toku monitoringu (czas i miejsce przechowywania, procedury reakcji na incydenty, ewaluacja poziomu wyszkolenia personelu). Aspekt funkcjonalny – ocena działania systemu w różnych warunkach (oświetlenia, atmosferycznych, etc.)
Wywiad gospodarczy	Ogólny zarys — opis Wskazania dotyczące — funkcjonalności zagrożenia,	Ocena zagrożeń wynikających z prowadzenia wywiadu gospodarczego Ocena wrażliwości na prowadzenia działań wywiadowczych	Prezentacja znanych sposobów pozyskiwania informacji gospodarczych.	Metody pozyskiwania informacji gospodarczych obejmują następujące bloki tematyczne: a. współczesne i historyczne paradygmaty praktyki wywiadu gospodarczego, b. formalizacja i standaryzacja procedur działań wywiadowczych prowadzonych w i poza przedsiębiorstwami (paradygmat *Competitive Intelligence*),

	podatności na działania wewnętrzne i zewnętrzne			c. metodyka pozyskiwania informacji gospodarczych – infobrokering cyfrowy (dane elektroniczne, Internet powierzchniowy i głęboki, intranety i ekstranety jako źródła danych) oraz infobrokering klasyczny (niezdigitalizowane źródła danych), d. metodyka pozyskiwania i analizy informacji gospodarczych - ilościowe (podejście klasyczne – opisowe i indukcyjne oraz *data mining*) i jakościowe metody analizy rynku i konkurencji, badania porównawcze (*benchmarking*), e. technologiczne aspekty pozyskiwania informacji gospodarczych: oprogramowanie i aplikacje.
			Ocena zabezpieczenia kontrwywiadowczego	Ocena zabezpieczenia kontrwywiadowczego pozwoli na określenie jakości, poziomu i ewentualnych problemów w zakresie poziomu zabezpieczenia dorobku intelektualnego przedsiębiorstwa. Rekomendujemy przeprowadzenie jej metodą *desk research,* która ma długą tradycję w postępowaniu badawczym i śledczym. Polega na systematycznej, wielowymiarowej ilościowo-jakościowej analizie zgromadzonego materiału: dokumentów oraz procedur i schematów działania. Poprowadzona zostanie w dwóch wymiarach: statycznym, polegającym na analizie dokumentów zastanych zawierających treści i procedury w zakresie bezpieczeństwa informacyjnego przedsiębiorstwa (akty prawne i para-prawne) oraz w aspekcie dynamicznym umożliwiającym ocenę faktycznego funkcjonowania przedsiębiorstwa w sferze bezpieczeństwa informacyjnego.
			Ocena możliwości pozyskania pracowników firmy przez firmy prowadzące wywiad	Weryfikacja metodą *mystery calling* (np. *mystery caller* w roli pracownika firmy headhunterskiej) stopnia satysfakcji pracowników z wykonywanej pracy/skłonności do skorzystania z innych ofert z przyczyn finansowych. W szczególności takiej procedurze rekomendujemy poddać pracowników o kluczowych kompetencjach technicznych/merytorycznych oraz pracowników dysponującymi kluczowymi informacjami. Określenie podatności pracowników na inżynierię społeczną (fałszywe wiadomości e-mail wyłudzające informacje, podszywanie się pod zwierzchników w rozmowach telefonicznych, etc.)
			Biały wywiad - zobrazowanie dotychczas dostępnych informacji znajdujących się w domenie publicznej	Analiza zawartości informacji znajdujących się w domenie publicznej obejmie następujące elementy: a. analizę treści zasobów Internetu (informacji na temat przedsiębiorstwa dostępnych w portalach i wortalach ogólnotematycznych oraz branżowych, informacji dostępnych w mediach społecznościowych, zasobów sieci 1.0 - stron internetowych oraz forów internetowych, w tym zamkniętych forów, artykułów i komentarzy w serwisach dziennikarstwa obywatelskiego

				polskich i zagranicznych. Przeprowadzona zostanie również analiza historycznych (lub usuniętych) informacji znajdujących się w Internecie (wykorzystanie Internet Wayback Machine)). b. analizę treści zasobów "tradycyjnych" mediów (analiza zawartości prasy na podstawie dostępnych archiwów elektronicznych artykułów prasowych). Cezury analiz zostaną ustalone w toku rozmów ze Zleceniodawcą w zależności od jego zapotrzebowań.

Standardowy raport z dokonanych czynności zawiera:

–Analizę zastanego zabezpieczenia pomieszczeń przed inwigilacją prowadzona przy pomocy środków technicznych wraz ze skanami mierzonych częstotliwości oraz propozycję zabezpieczenia pomieszczeń.

–Analizę opracowanych scenariuszy zamachów wraz z oceną podatności na ataki wewnętrzne/sabotaż oraz rekomendacje poprawy sytuacji.

–Analizę słabych/mocnych stron ochrony technicznej – umiejscowienie CCTV, barier, środków ochrony technicznej wraz z propozycjami zmian.

Efektem podjętych działań będzie raport syntetycznie prezentujący ewentualne luki w istniejących zabezpieczeniach fizycznych oraz informacyjnych. Integralną część raportu stanowią wskazówki w zakresie rekomendowanych działań kontrwywiadowczych oraz sugerowanych środków bezpieczeństwa.

4. Usługi detektywistyczne

Oferujemy zarówno klasyczne usługi detektywistyczne, takie jak obserwacja wskazanej w umowie osoby. Dyskretna obserwacja prowadzona przez doświadczonych detektywów przy użyciu nowoczesnego sprzętu do nagrywania video i robienia zdjęć. Po zakończeniu usługi Klient otrzymuje pełne i szczegółowe pisemne sprawozdanie wraz z dowodami w postaci zdjęć oraz nagrań video obserwowanych osób. Oferujemy również usługi nowatorskie – biały i szary wywiad w Internecie oraz *mystery calling*.

4.1. Biały i szary wywiad w internecie.

Usługi infobrokerskie obejmują profesjonalne i skuteczne tworzenie dossier firmy lub innego podmiotu na podstawie danych znajdujących się w powierzchniowym i ukrytym (komercyjne i niekomercyjne bazy i hurtownie danych, rejestry, archiwa) Internecie. Ogniskuje się na wyszukiwaniu, selekcjonowaniu i dostarczaniu zadanych przez Klienta informacji. Nie sprzedajemy informacji, lecz swoje umiejętności w zakresie ich odnalezienia. Usługa obejmuje również analizę dokumentów przedsiębiorstwa oraz badanie klimatu opinii w Internecie (media społecznościowe) na temat przedsiębiorstwa lub innego podmiotu. W tym zakresie możliwa analiza jakościowa (analiza wydźwięku vel sentymentu, inne analizy jakościowe) oraz ilościowa (pełny zakres analiz statystycznych: statystyka opisowa i indukcyjna). Zdobywamy informacje, które na ogół są pomijane przez wywiadownie gospodarcze i w tym rozumieniu infobrokering stanowi uzupełnienie białego wywiadu rynkowego.

W szczególności oferujemy monitoring podatności na elektroniczny biały wywiad obejmujący ewaluację zakresu i treści informacyjnych generowanych przez podmiot oraz wynikających zagrożeń informacyjnych w Internecie. Analiza prowadzona jest w następujących aspektach:

- przedmiotowym (otoczenie zewnętrzne i wewnętrzne przedsiębiorstwa ze wskazaniem na instytucje oraz procesy),

- podmiotowym (pracownicy, kontrahenci, dostawcy).

Postępowanie analityczne obejmuje:

- Sieć 1.0

- Sieć 2.0 (z uwzględnieniem dziennikarstwa oddolnego – *grassroot reporting* i blogosfery)

- na życzenie Sieć 0.0 oraz tzw. Ukryty Internet.

Wyniki prezentowane są w formie opisowej, tabelarycznej, statystyk opisowych i indukcyjnych oraz syntetycznych wskaźników analizy wydźwięku (*sentiment analysis*) przyjętej i ugruntowanej na potrzeby analizy treści medialnych. Zakres usług może objąć również działania z użyciem wirtualnych marionetek (*sockpuppets*) służących między innymi do sprawdzania lojalności pracowniczej.

Cena:
Wycena indywidualna, do uzgodnienia w zależności od zakresu i zapotrzebowań Klienta

4.2. Mystery calling

Profesjonalne usługi telefoniczne w zakresie sprawdzania centrów obsługi telefonicznej, wartowni, departamentów/działów bezpieczeństwa przedsiębiorstw i instytucji, sekretariatów i innych komórek polegających na kontakcie telefonicznym jako jednej z form komunikowania się z otoczeniem. Mamy możliwość zastrzegania/zmieniania numerów telefonicznych, pracujemy na podstawie szczegółowo przygotowane scenariusze zdarzeń oraz starannie zapamiętane i przećwiczone „legendy" telefonujących, dysponujemy kilkunastoosobowym zespołem wyszkolonych *mystery callerów.*

Cena:
Wycena indywidualna, do uzgodnienia w zależności od zakresu i zapotrzebowań Klienta

5. Szkolenia

Oferujemy szereg autorskich, unikatowych szkoleń. Prowadzą je emerytowani oficerowie i inni funkcjonariusze służb dyspozycyjnych, wykładowcy Uniwersytetu Warszawskiego, Warszawskiego Uniwersytetu Medycznego oraz eksperci w zakresie ratownictwa medycznego i instruktorzy samoobrony z wieloletnim stażem.

Nasza oferta szkoleniowa obejmuje obecnie:

5.1. Wstępne szkolenie z zakresu unikania podsłuchów

Czas trwania: ok. 120 minut

Proponowany zakres szkolenia:

1.Zasady postępowania podczas rozmów biznesowych prowadzonych poza budynkiem firmy.

a)Postępowanie z telefonami komórkowymi i laptopami.

b)Zasady rozmów prowadzonych poza obiektami firmy.

2.Pokaz urządzeń podsłuchowych.

3.Metody i urządzenia stosowane do wykrywania podsłuchu.

Cena:
Do ustalenia indywidualnie oraz ewentualne koszty dojazdu, pobytu, wynajęcia sali, cateringu.

5.2. Bezpieczna komunikacja przez telefon i Internet. Jak nie dać się zhakować lub podsłuchać?

Czas trwania części teoretycznej – 6 godzin zegarowych, ćwiczenia – 6 godzin zegarowych

Przegląd zagrożeń bezpieczeństwa komunikacji. Metody kradzieży tożsamości i naruszania prywatności: luki bezpieczeństwa aplikacji, ataki *man in the middle*, wirusy, robaki, exploity i rootkity, metadane plików, odgadywanie prostych haseł, keyloggery programowe. Człowiek jako najsłabsze ogniwo (*phishing* / *spearphishing*). Autorski przegląd

programów naruszających prywatność: od Netbusa i Prosiaka do VNC, RDP i pcAnywhere. Kali Linux – analiza możliwości najpotężniejszego narzędzia hakerskiego.

Zabezpieczanie komputerów i innych urządzeń połączonych z Internetem. Podstawy bezpiecznej i anonimowej komunikacji: zmiana adresu IP, MAC adresu kart sieciowych, wykorzystanie anonimowych proxy i VPN, użycie trasowania cebulowego (TOR), komunikacja *via* I2P (Invisible Internet Project) oraz Zeronet. Freenet oraz Freenet w trybie Darknet – narzędzie konspiratorów. Anonimowy e-mail (Protonmail, Mailvelope, tymczasowe i losowo generowane skrzynki e-mail). Bezpieczny chat. Anonimowi w Internecie – wirtualizacja systemu operacyjnego i programów, bootowalny nośnik z systemem operacyjnym (instruktaż używania Linux Tails). Generowanie fałszywych tożsamości *ad hoc*, hodowla fałszywych tożsamości (*sockpuppets*), kupno fałszywych tożsamości.

Zabezpieczanie telefonów komórkowych. Metody podsłuchu telefonów komórkowych (warstwa GSM i innych protokołów komunikacyjnych, warstwa aplikacji). Podsłuch telefonów komórkowych – jak robią to profesjonaliści: ataki „cichych smsów", ataki z użyciem protokołu SS7, ataki na karty sim z użyciem specjalnie spreparowanych wiadomości sieci, użycie *IMSICatcherów*. Dedykowane programy umożliwiające podsłuch: *Remote Control System, DaVinci, Galileo*. Bezpieczny system operacyjny (zabezpieczenie smartfonów z systemem Android). Przegląd systemów bezpiecznych (PrivOS). Bezpieczne korzystanie z Internetu w smartfonie: podstawy oraz elementy zaawansowane – Orbot i Orfox. Bezpieczny sms (Signal Private Messenger), bezpieczny chat (np. chat.onion). Rozmowy telefoniczne bez podsłuchu Red Phone (+OnSip / Iptel). Bezpieczna komunikacja z BTS. Warsztaty: diagnostyka oraz zabezpieczenie własnych telefonów.

Cena:
W zależności od zakresu.

5.3. Bezpieczne przechowywanie informacji (komputer i smartfon). Jak zachować swoją prywatność?

Czas trwania części teoretycznej – 6 godzin zegarowych, ćwiczenia – 6 godzin zegarowych

Techniki pozyskiwania jawnych i ukrytych danych systemowych. Dane jawne: poczta – analiza nagłówków e-mail, dokumenty elektroniczne, pliki tymczasowe, partycje i pliki wymiany, pliki kopii, logi i rejestry, dane przeglądarki, pliki kolejkowania wydruku, ciasteczka i sygnalizatory sieci). Dane ukryte: metadane, dane skasowane, slack space, RAM-slack. Przegląd wybranych programów przeznaczonych do informatyki śledczej. Oprogramowanie *open source*: The Sleuth Kit, Foremost, Scalpel, Photorec, Regripper, Pasco. Oprogramowanie komercyjne: Cofee, X-ways Forensics. Kwestie prawne: tzw. paragrafy hakerskie w Kodeksie Karnym (art. 267, 269a i 269b). Pozyskiwanie danych bez umiejętności informatycznych: inżynieria społeczna.

Zagrożenie inwigilacją *offline*. Odnajdywanie zgubionych/zapomnianych haseł do plików (narzędzie Cain&Abel). Pozyskiwanie dostępu do systemu operacyjnego bez hasła. Keyloggery sprzętowe. Metody zaawansowane łamania prywatności: przechwytywanie emisji elektromagnetycznej, podsłuch laserowy, emisja radiowa, emitowane ciepło, technologia ultradźwięków.

Sprzątanie po sobie elektronicznych śmieci i zacieranie śladów. Metadane – cichy zabójca prywatności. Metody zautomatyzowanego usuwania metadanych. Czyszczenie pamięci podręcznej i innych śladów. Ukrywanie informacji w plikach: steganografia, steganofonia, steganowizja. Kilka słów o hasłach. Jak skutecznie pozbyć się danych (od metod fizycznych do chemicznych)? Ukrywanie i szyfrowanie plików i katalogów (VeraCrypt *versus* BitLocker i inne programy szyfrujące). Poziomy szyfrowania: plik, katalog, cały system operacyjny.

Cena:
W zależności od zakresu.

5.4. Skuteczne pozyskiwanie i techniki oceny wiarygodności informacji

Czas trwania części teoretycznej – 240 minut, ćwiczenia – 180 minut

Typologia źródeł informacji. Ujęcie przedmiotowe źródeł danych: media „klasyczne", publicznie dostępne rejestry i ewidencje, Internet jako źródło informacji. Ujęcie podmiotowe źródeł danych: instytucje państwowe lub z udziałem Skarbu Państwa (I sektor), podmioty komercyjne (II sektor), Podmioty *non-profit* (NGO's, III sektor). Osobowe źródła informacji. Wywiad gospodarczy i paradygmat *competitive intelligence.*

Techniki i taktyki ewaluacji wiarygodności informacji. Paradoksy i meandry ludzkiej pamięci: ograniczone przetwarzanie bodźców, efekt błędnej informacji, obronność percepcyjna, amnezja psychogenna, pamięć generatywna. Wiarygodność świadków. Anatomia kłamstwa. Sztuka skutecznego kłamstwa. Wykrywanie kłamstwa. Zasady i sposoby pozyskiwania prawdy (od psychologicznych sztuczek do wariografu, skopolaminy i tortur). Źródła rzeczowe informacji. Taktyki i techniki przesłuchań. Gry informacyjne – kształcenie praktycznych umiejętności zdobywania informacji i wyciągania wniosków (gra w Mafię – Dymitra Dawidowa).

Cena:
W zależności od zakresu.

*5.5. Środki i metody **inwigilacji** elektronicznej – wykład poglądowy*

Czas trwania: 180 minut

Typologia stanów bezpieczeństwa informacyjnego. Autorska typologia ryzyk utraty informacji. Studia przypadków utraty informacji – szpiegostwo przemysłowe. Studia przypadków i utraty informacji – szpiegostwo polityczne. „Ojciec" podsłuchów – „Złotousty" 1945/1952. Polskie „afery podsłuchowe": Restauracja „Sowa i Przyjaciele" / Pałac Sobańskich, Restauracja „Różana", „Afera taśmowa" Renaty Beger. Studium przypadku zaawansowanej gry operacyjnej – Gazociąg Transsyberyjski, 1982.

Typowe miejsca i sposoby inwigilacji. Urządzenia i oprogramowanie szpiegowskie. Minikamery i rejestratory audio/wideo (fotopułapki, minikamery ukryte, minirejestratory audio/video). Lokalizatory GPS (lokalizacja na bieżąco, lokalizacja przedmiotów, zapis trasy GPS). Podsłuch i lokalizacja telefonu (oprogramowanie, sprzęt). Podsłuchy i odbiorniki (podsłuchy klasyczne, podsłuch GSM dużego zasięgu, podsłuchy sejsmiczne, skanery, mikrofony paraboliczne, mikrofony laserowe. Wykrywacze kamer i podsłuchów (wykrywacz podsłuchów, wykrywacze kamer, wykrywacze uniwersalne). Generatory szumu / zagłuszacze (szyfrowanie rozmów telefonicznych, *scrambler*). Gadżety szpiegowskie i ciekawostki (modulator głosu, SIM Recovery Pro). Wykrywacze substancji chemicznych (detektor materiałów wybuchowych i narkotyków, wykrywacz przemytu, znakowanie przedmiotów). Metody inwigilacji *offline*: emisja elektromagnetyczna, podsłuch laserowy, emisja radiowa, emitowane ciepło, technologia ultradźwięków.

Cena:
W zależności od zakresu.

5.6. Metodyka pozyskiwania wiedzy i analizy informacji

Czas trwania części teoretycznej – 6 godzin zegarowych, ćwiczenia – 6 godzin zegarowych

Podejście ilościowe w pozyskiwaniu informacji. Podejście jakościowe w pozyskiwaniu informacji. Podejście mieszane (ilościowo-jakościowe) w pozyskiwaniu informacji. Analiza danych: techniki ilościowe, techniki jakościowe. Metoda delficka. Burza mózgów (brainstorming), w tym odmiany burzy mózgów (Indywidualna BM, Technika 635, Philips 66 Buzz Session). Synektyka W.J.J. Gordona. Metoda morfologiczna. Techniki CERMA. Metoda scenariuszowa. Metody „analogowe". Forecasting i foresighting. Metody symulacyjne. Metody „liczbowe": reguła „kciuka", reguła Pareto, test Grafa, kryterium Chauveneta, prawo Benforda. Gry symulacyjne i decyzyjne (serious games).

Praktyczne aspekty wyboru i oceny operatów losowania. Typy reprezentatywności i metody jej zapewnienia. Wielkość próby a rozkład normalny. Obliczanie minimalnej wielkości próby. Maksymalny standardowy błąd oszacowania (msbo) – obliczanie. Modyfikacje msbo (poprawka Cochrana). Zastosowanie i interpretacja msbo. Wzór uproszczony na msbo. Test losowości próby (serii/Stevensa/Walda-Wolfowitza), czyli jak ujawnić cykliczność w zbiorze danych. Problem pseudoprzedziału ufności Grzegorza Lissowskiego. Poziomy pomiaru - skala S.S. Stevensa. Interpretacje danych tabelarycznych (tabele jedno- i wielozmiennowe). Interpretacje miar statystyki opisowej. Wybrane miary tendencji centralnej: średnie (arytmetyczna oraz inne: ważona, odcięta, winsorowska, krocząca), dominanta, mediana, skośność i kurtoza. Wybrane miary dyspersji: wariancja i odchylenie standardowe. Interpretacje miar statystyki indukcyjnej. Wybrane miary związku między zmiennymi: współczynnik korelacji R Pearsona, eta (η), chi-kwadrat (χ^2) Pearsona, współczynnik kontyngencji C Pearsona, współczynnik V Craméra. Badanie różnic między dwiema grupami na przykładzie testu t-Studenta. Interpretacja testu Kruskala-Wallisa i U Manna-Whitney'a. Zaawansowane metody analizy: CATREG.

Cena:
W zależności od zakresu.

5.7. Biały, szary i czarny wywiad w Internecie

Czas trwania części teoretycznej – 6 godzin zegarowych, ćwiczenia – 6 godzin zegarowych

Topografia Internetu. Wyszukiwanie w Google. Zasady indeksowania i pozycjonowania w wyszukiwarce Google (PageRank). Mechanizmy modyfikujące PageRank (szkic). Wyszukiwanie z użyciem Google: znaki Boole'a (+, -, „"), wybrane operatory (stop words, site, filetype, intitle, intext, ~ (tylda), related, operatory zakresowe (.., *), operatory informacyjne (define, info, cache, link). Przegląd wyszukiwarek internetowych. Metawyszukiwarki i multiwyszukiwarki. Wyszukiwarki naturalne. Katalogi internetowe. Wyszukiwarki ludzi. Archiwa Internetu (WayBackMachine). Inne wyszukiwarki (naukowe, domen, etc.). Wyszukiwanie w Sieci 2.0 – blogów, wyszukiwanie w sieciach społecznościowych i forach dyskusyjnych. Delokalizacja wyników wyszukiwania.

Zaawansowane techniki wyszukiwania – Google, Yandex, Bing, DuckDuckGo Hacking. Google Hacking Database. Google Hacking jako biały, szary i czarny wywiad. Biały wywiad: wyszukiwanie stron usuniętych i archiwalnych, wyszukiwanie niektórych informacji o użytkownikach oraz innych informacji merytorycznych. Szary wywiad: zdobywanie informacji pozostawionych (nieświadomie) przez twórców i właścicieli witryn internetowych, informacji o strukturze witryn internetowych oraz parametrów konfiguracyjnych serwerów www. Czarny wywiad: potencjał uzyskiwania informacji zabezpieczonych, osobowych danych wrażliwych oraz parametrów konfiguracyjnych programów i urządzeń.

Tworzenie zapytań prostych i złożonych, porównywanie wyników wyszukiwań, praktyczne poznawanie ograniczeń i możliwości poszczególnych wyszukiwarek internetowych, empiryczne zweryfikowanie hipotezy *filter bubble*.

Narzędzia do masowego przeszukiwania Internetu: Oryon OSINT Browser, Maltego Paterva. Charakterystyka funkcjonalna i techniczna. Instalacja i konfiguracja. oprogramowania Zautomatyzowane sposoby pozyskiwania informacji. Eksploracja Internetu Rzeczy (Internet of Things) – Shodan i Censys. Charakterystyka. Sposób używania. Filtry.

Eksploracja ukrytych Internetów. Charakterystyki techniczne i funkcjonalne TOR (*The Onion Router*), Freenet, I2P (*Invisible Internet Project*), Zeronet. Alternatywne światy – OpenNIC. Instalacja i konfiguracja. Zasady bezpiecznego korzystania. Wyszukiwarki, katalogi i charakterystyka zasobów.

Cena:
W zależności od zakresu.

5.8. Tajniki Internetów

Czas trwania: 180 minut

Internet czy Internety?

Od Sieci 0.0 do Sieci 5.0. Czy za swojego życia zawrzesz znajomość z myślącym i czującym programem?

Zasoby niewidoczne w Google – dlaczego przeciętny użytkownik Internetu ma dostęp do tylko jednego procenta zasobów Internetu?

Sztuka wyszukiwania w Google – *Google Hacking*/*Google Dorks*. Google jako cudowna broń – od wyszukiwania stron usuniętych i archiwalnych do wyszukiwania kamer i haseł użytkowników.

Jak skutecznie inwigilować swoich (nie)przyjaciół? Wprowadzenie do Maltego i Oryon OSINT Browser. Kilka słów o wirtualnych marionetkach (*sockpuppets*).

Dlaczego bać się Internetu Rzeczy (*Internet of Things*)? Co nieco o niektórych narzędziach podglądaczy i cyberterrorystów (Shodan, Censys).

Dinozaury Internetu, czyli o tym, co było przed www (wybrane przykłady: BBS/Fidonet, Gopher, Usenet, niespełnione marzenie –Xanadu).

Alternatywny wszechświat. Internet istniejący obok powszechnie znanego – OpenNIC (*Alternative Top Level Domain*).

Jak znaleźć to, czego lepiej nie widzieć (*The Onion Router*), czyli rzecz o Ukrytym/Głębokim Internecie (*Deep Web, Hidden Web*), gdzie odnajdziemy czarny i

czerwony rynek (handel bronią, żywym towarem, narkotykami i płatnych zabójców...). Słowo o równie złych braciach TORa – I2P (*Invisible Internet Project*) i Freenet[2].

Cyberhigiena... czyli jak się skutecznie zabezpieczyć korzystając z Internetu? Anonimowi w Internecie – czy wystarczy Linux Tails? Kilka słów o hasłach. Bezpieczny e-mail. Człowiek jako najsłabsze ogniwo (*phishing* / *spearphishing*). Jak skutecznie pozbyć się danych? O szyfrowaniu danych.

Cena:
W zależności od zakresu.

2 Wyłącznie dla słuchaczy o mocnych nerwach!

5.9. Terroryzm przemysłowy

Czas trwania: 120 minut

Tło globalne – statystyki. Terroryzm w Europie. Zagrożenia obiektów przemysłowych: występek chuligański, napad rabunkowy, kradzież, sabotaż/zemsta, cyberterroryzm, terroryzm, wojna hybrydowa. Szacowanie ryzyka. Analiza przypadków terroryzmu przemysłowego.

Cena:
W zależności od zakresu.

5.10. Taktyka i procedury bezpieczeństwa

Czas trwania: ok. 3 x 55 minut, wykład z prezentacją, 55 minut – ćwiczenia praktyczne w postaci symulacji napadu i odbicia zakładników

Merytoryczne cele szkolenia obejmą:

- ilościowo-jakościową analizę zjawiska przestępczości w perspektywie porównawczej: globalnej, europejskiej i polskiej;
- zapoznanie uczestników szkolenia z zakresem i treścią pojęcia przestępczości, jego rozumieniem akademickim;
- publicystycznym i potocznym oraz uporządkowanie subpojęć dotyczących zjawiska przestępczości: jego typów i klas;
- ewaluację zagrożeń przestępczością na terenie Polski

Praktyczne cele szkolenia obejmą:

- zaopatrzenie w wiedzę dotyczącą rozpoznawania zagrożeń atakiem, kradzieżą.
- ewaluację zagrożeń bronią palną, białą i innymi przedmiotami niebezpiecznymi oraz zasady postępowania w sytuacji szantażu lub ataku nimi;
- zasady podstawowej samoobrony;
- zasady zachowania się podczas sytuacji zakładniczej.

Zakres merytoryczny szkolenia

- sztuka obserwacji i interpretacji sygnałów potencjalnego incydentu bezpieczeństwa
- socjopsychologiczne reguły skutecznego wzywania pomocy.
- zachowanie podejrzane.
- reguły zachowania w zależności od sprawców ataków. Jak nie dopuścić do ataku.
- zagrożenie przestępczością – Statystyki przestępczości.
- zasady zachowania się w sytuacji kryzysu zakładniczego/napadu – **symulacja napadu.**

- podstawy samoobrony.

Cena dla grupy do 25 osób:
W zależności od zakresu. Szacunkowo: 1500PLN/godz. oraz ewentualne koszty dojazdu, pobytu, wynajęcia sali, cateringu. Dokładna wycena ustalana jest indywidualnie.

5.11. Samoobrona

Najbardziej efektywną formą realizacji tej tematyki są dwudniowe zajęcia wyjazdowe. Jednak, na życzenie klienta możliwe jest również przeprowadzenie zajęć stacjonarnych.

Pierwszy dzień:

Czas zajęć 10 godzin.

1. Psychologiczne umiejętności do obrony – unikanie „bycia ofiarą".

- sposoby unikania zagrożenia.
- samoświadomość, intuicja
- asertywność, stawianie granic, komunikacja niewerbalna.
- opanowanie emocji w czasie bezpośredniego zagrożenia;

2. Portret psychologiczny typowego napastnika.
3. Proces „typowania ofiary".
4. Oznaki agresji wynikające z zachowania agresora.

- agresja niejawna;
- agresja jawna

Dzień drugi:

- Czas zajęć 8 godzin lekcyjnych.
- Portret pamięciowy – 1h;
- Samoobrona w przypadku napadu -4h;

W ramach zajęć z samoobrony, omówienie różnych rodzajów broni, w tym broni palnej. Sposoby jej użycia do samoobrony oraz obrona przed atakiem. Nauka najbardziej skutecznych uderzeń i kopnięć, wykorzystania do obrony przedmiotów znajdujących się w otoczeniu ofiary.

Umiejętność improwizacji. Obserwacja otoczenia. Zajęcia są prowadzone na sali treningowej, i w „terenie".

- Pierwsza pomoc przedmedyczna – 3h

Uwagi:

Tematyka zajęć może być zmieniona i dostosowana do życzeń klienta.

Cena
Koszt zajęć zależy od liczby osób, oraz miejsca organizacji zajęć. Możliwe zajęcia indywidualne.

6. Uwagi

1.*Podane ceny są cenami NETTO w PLN.*

2.*Jeśli zlecenia ma być wykonane poza Warszawą, do ceny doliczamy koszt dojazdu i ewentualnego pobytu.*

3.*Zgodnie z art. 178 ust. 3 Prawa telekomunikacyjnego, zagłuszanie pasma telefonów komórkowych jest zabronione z wyłączeniem podmiotów wyszczególnionych w art. 4 Prawa telekomunikacyjnego na podstawie art. 178 ust. 3 Prawa telekomunikacyjnego. Prowadzimy sprzedaż zagłuszaczy TYLKO dla uprawnionych instytucji.*

4.*Koszt zabezpieczenia pomieszczenia o powierzchni 50m2 wynosi ok. 70 000zł netto, jednak dokładny koszt określany jest zawsze po przeprowadzeniu wizji lokalnej.*

5.*Koszty montażu ustalamy po przeprowadzeniu wizji lokalnej i określeniu zakresu prac.*

6.*Oferta jest ważna 30 dni.*

Sekkura Sp. z o.o.
Paweł TOMCZYK
Członek Zarządu