

## Security/Warsztaty z Cyberbezpieczeństwa



### PRZEZNACZENIE SZKOLENIA

Szkolenie skierowane do kadry zarządzającej oraz pracowników administracyjnych, użytkowników komputerów i innych urządzeń z dostępem do Internetu, nie będących specjalistami z zakresu bezpieczeństwa IT.

### KORZYŚCI WYNIKAJĄCE Z UKOŃCZENIA SZKOLENIA

Poszerzenie wiedzy pracowników na temat bezpiecznego korzystania z cyberprzestrzeni w miejscu pracy i poza nim.

Uczestnicy nauczą się:

- definiować i charakteryzować najważniejsze techniki cyberataków,
- rozpoznawać i zapobiegać zagrożeniom związanym z cyberprzestępczością,
- podejmować odpowiednie działania (zabezpieczenia) w przypadku usiłowania cyberataku,
- rozpoznawać socjotechniki wykorzystywane przez „ cyberprzestępców”,
- docelowo także popularyzować wiedzę nabytą na szkoleniu w organizacji.

### OCZEKIWANE PRZYGOTOWANIE SŁUCHACZY

Wymagana ogólna wiedza informatyczna z zakresu systemów operacyjnych i zagadnień sieciowych.

**Jako uzupełnienie rekomendujemy:**

Praktyczny trening zasad bezpieczeństwa informacji w firmie - Symulacja biznesowa „Ambasada”.

## AGENDA SPOTKANIA

Sala szkoleniowa

### 1. Wstęp

- Co to jest cyberbezpieczeństwo - definicja cyberprzestrzeni i cyberbezpieczeństwa, dlaczego to jest ważne
- Ryzyko i zarządzanie ryzykiem - co to jest ryzyko, podstawowe pojęcia i zasady zarządzania ryzykiem
- Polityka bezpieczeństwa - czym jest w organizacji polityka bezpieczeństwa i jaka jest jej rola
- Incydenty bezpieczeństwa - co należy rozumieć jako incydent bezpieczeństwa i jak z nim postępować
- Normy i standardy bezpieczeństwa - powszechnie stosowane rozwiązania, norma ISO27001

### 2. Ataki „na człowieka” tzw. SOCJOTECHNIKA (stosowane techniki manipulacji)

- Ataki socjotechniczne - techniki manipulacji wykorzystywane przez cyberprzestępców
- Sposoby - pod jakimi pretekstami wyłudza się firmowe dokumenty
- Wykrywanie - jak rozpoznać, że jest się celem ataku socjotechnicznego
- Reakcja - jak prawidłowo reagować na ataki socjotechniczne
- Jak i skąd atakujący zbierają dane na twój temat
- Miejsca, w których zostawiamy swoje dane świadomie i nieświadomie - jak świadomie udostępniać informacji w sieci

### 3. Atak „na komputery” - demonstracje wraz z objaśnieniem metod ochrony

- Przegląd aktualnych ataków komputerowych wykorzystywanych przez cyberprzestępców, typowe błędy zabezpieczeń wykorzystywane przez atakujących
- Ataki przez sieci bezprzewodowe (WiFi, Bluetooth, NFC)
- Ataki przez pocztę e-mail (fałszywe e-maile)
- Ataki przez strony WWW - jak nie dać się zainfekować, fałszywe strony
- Ataki przez komunikatory (Skype, Facebook)
- Ataki przez telefon (fałszywe SMS-y, przekierowania rozmów, itp.)
- Ataki APT, phishing, smishing, spear-phishing, pharming, spoofing, spam, spim, scam

### 4. Dobre praktyki związane z bezpiecznym wykorzystaniem firmowych zasobów

- Polityka haseł, zarządzanie dostępem i tożsamością - jakie hasło jest bezpieczne, jak nim zarządzać, zasady udzielania dostępu do zasobów informacyjnych
- Bezpieczeństwo fizyczne - urządzenia, nośniki danych, dokumenty, „czyste biurko”
- Bezpieczna praca z urządzeniami mobilnymi (smartfon, tablet, laptop)
- Problem aktualnego oprogramowania i kopii zapasowych
- Bezpieczna praca z pakietem biurowym Microsoft Office
- Bezpieczna praca z programem pocztowym
- Bezpieczna praca z przeglądarką internetową
- Zastosowanie technik kryptograficznych (szyfrowanie, certyfikaty)

### 5. Aspekty prawne

- Odpowiedzialność pracownika przed pracodawcą za ujawnienie informacji
- Nieautoryzowane użycie systemów komputerowych
- Rażące zaniedbania związane z wykorzystywaniem sprzętu komputerowego
- Dane osobowe i dane wrażliwe

---

|                      |                     |
|----------------------|---------------------|
| <b>Kod szkolenia</b> | BS.IT CS / PL AA 2d |
| <b>Czas trwania</b>  | 2 dni               |
| <b>Poziom</b>        | Podstawowy          |
| <b>Autoryzacja</b>   | Altkom              |