Bezpieczeństwo cybernetyczne – ochrona tajemnicy adwokackiej i obrończej.

Głównym celem szkolenia jest budowanie wśród pracowników Kancelarii świadomości płynących z zagrożeń cybernetycznych, mogących w pośredni lub bezpośredni sposób naruszyć ochronę tajemnicy adwokackiej lub obrończej.

Na konkretnych przykładach szkolenie obrazuje z jakich narzędzi i technik korzystają cyber przestępcy w celu naruszenia struktury bezpieczeństwa kancelarii.

Efektem szkolenia jest uszczelnienie sytemu bezpieczeństwa poprzez podniesienie umiejętności zespołu oraz raport, adresujący najważniejsze kwestie bezpieczeństwa cybernetycznego. Elementem dodatkowym jest również zbudowanie świadomości w zakresie cyber przestępczości, jako zjawiska będącego częścią obecnej kryminologii.

Czas trwania : 3h

Cena obejmuje przygotowanie raportu końcowego, stanowiącego podsumowanie programu szkolenia. Przedstawia on obraz poziomu wiedzy pracowników i adresuje potencjalne miejsca do przyszłych działań z zakresu bezpieczeństwa cybernetycznego.

Program szkolenia:

1. Wprowadzenie – cyber zagrożenia

- omówienie cyberprzestępczości na podstawie przypadków znanych z mediów;
- cele ataku.

Punkt ten ma na celu wprowadzenie szkolonej grupy w konkretny styl myślenia o zagrożeniach cybernetycznych i możliwościach, jakimi dysponują cyber przestępcy, a także określenia, co może stać się przedmiotem ataków. W celu zobrazowania zagrożeń opieramy się na przykładach, z którymi spotkaliśmy się w trakcie pracy i takich, które były początkiem sytuacji kryzysowych, na które reagowaliśmy.

2. Źródła zagrożeń:

a. Mail, www – jak narzędzia codziennej wymiany informacji mogą być wykorzystane przeciwko nam:

- Spam;
- Phishing;
- Malware;
- Cryptolocker.

Sekcja ta skupia się na konkretnych narzędziach, używanych w celach ataku na wizerunek i reputację firmy, na blokowanie lub utrudnienia komunikacji. Dodatkowo szkolimy jak rozpoznawać i reagować na próby wyłudzenia danych i podszywania się np. pod naszą firmę lub bank, jak nie paść ofiarą złośliwego oprogramowania szpiegującego lub kradnącego dane oraz jak chronić dane przed cyber szantażem.

b. Media społecznościowe – jak ochronić swoją prywatność

- kradzież tożsamości;
- publikowanie informacji prywatnych;
- bezpieczna rodzina w internecie.

W sekcji tej nauczymy Państwa jak korzystać z mediów społecznościowych nie narażając się na kradzież tożsamości albo ataki na naszą reputację, jak zarządzać informacjami jakie publikujemy w sieci i jak sprawić, by nie wpadły w niepowołane ręce. Skupimy się też na narzędziach, które mają służyć cyber ochronie członków rodziny, gdyż wiele ataków wymierzonych w naszych klientów zaczyna się od wykorzystywania ufności członków ich rodzin.

c. Hardware – urządzenie osobiste powinno być bezpieczne

- Smartfon, tablet;
- Komputer.

Sekcja ta obrazuje jak działają patologie wykorzystane przez cyber przestępców penetrujących sprzęty, których używamy w codziennym życiu. Sekcja obrazuje jak telefon z dostępem do internetu przekłada się na „dostęp internetu" do właściciela narzędzia typu smartfon, tablet. W trakcie szkolenia skupiamy się na przekazaniu praktycznej wiedzy z zakresu bezpiecznego wykorzystania narzędzi pracy, mogących być celem ataku.

d. Człowiek – najsłabsze ogniwo

- Socjotechnika stosowana;
- Inżynieria społeczna.

Sekcja ta skupia się na przedstawieniu niestarzejących się metodach ataków socjotechniczny oraz na jej rozwoju. Omawiamy działanie inżynierii społecznej i systemy ochrony przed jej użyciem.

3. Konsekwencje wynikające z cyberprzestępstw

- skutki zaniechań i świadomych działań pracowników.

Sekcja ta obrazuje kto, jak i dlaczego może narazić firmę na straty. Od niefrasobliwości aż po złą wolę pracowników. Sekcja obrazuje również dlaczego ważny jest background check przy zatrudnianiu na stanowiska IT.

4. **CyberBHP - jak być bezpiecznym**

- wzorce zachowań minimalizujące podatność na cyber zagrożenia.

> Sekcja ta obrazuje to, jak 20% dobrych praktyk zmniejsza o 80% szansę na zostanie ofiarą cyberataku. Wskazuje często popełniane błędy przy zbyt słabych ale też zbyt silnych zabezpieczeń w zakresie IT.

5. **Zabezpieczenie dowodu elektronicznego cyberprzestępstw na potrzeby postępowania sądowego**

   Uczestnicy szkolenia zdobędą wiedzę, jak zabezpieczyć możliwy materiał dowodowy, potwierdzający dokonanie czynów zabronionych - omówionych podczas szkolenia.

6. **Podsumowanie i sesja Q&A**