

Profesjonalna ochrona informacji – mit, czy konieczność, praktyczne wytyczne na co dzień dla pracowników firm.

Cele szkolenia:

- podniesienie świadomości załogi Firmy wobec szeregu współczesnych, nieznanych zagrożeń utraty czy modyfikacji informacji.
- zapoznanie pracowników z wieloma rodzajami zabezpieczeń i metod ochrony przed w/w rodzajami zagrożeń.
- zbudowanie samoświadomości pracowników prowadzącej do naturalnej i niewymuszonej ochrony informacji na co dzień, metodami poznanymi na tym szkoleniu.

Korzyści z uczestnictwa w szkoleniu:

Kurs umożliwia w nowatorski sposób skutecznie zmienić złe przyzwyczajenia pracowników w ochronie wszelkich informacji danej firmy.

- Wprowadzenie wśród pracowników firmy kultury tzw. korzystnych zachowań pro-bezpiecznych
- Pracownicy traktują poznane na tym szkoleniu dobre sposoby postępowania jako własne
- Zbudowanie odpowiedzialności w świadomości każdego pracownika Firmy za ochronę wszelkich cennych informacji, co znacznie odciąża tych, którzy z definicji zajmują się Ochroną Danych Osobowych lub Informacji Niejawnych
- Znaczne odciążenie sektora IT w promowaniu pro-bezpiecznych zachowań pracowników
- Zwiększenie bezpieczeństwa firmy oraz jej cennych aktywów
- Uzyskanie imiennych certyfikatów przez uczestników szkolenia

Business People Alignment



Uczestnicy szkolenia:

Szkolenie dedykowane jest do jednorodnych grup pracowniczych, osobno dla Kadry Zarządzającej oraz osobno dla Pracowników.

Szkolenie dla Kadry Zarządzającej jest rozszerzone o:

- wybrane aspekty efektywnego zarządzania podległymi pracownikami w aspekcie zagrożeń bezpieczeństwa informacji.

Omawiane są szczegółowo różne postawy psychologiczne ludzi oraz ich reakcje na zapowiedź zmian w pracy danej organizacji, a także praktyczne sposoby modyfikowania przez Kadrę Zarządzającą tych postaw tak, aby zmieniały się w świadome zachowania pro-bezpieczne.

Jednocześnie zmniejszona jest ilość szczegółowych wytycznych, przydatnych bardziej dla ogółu pracowników.

Szkolenie dla grup pracowniczych jest pozbawione w/w aspektów praktycznego zarządzania zasobami ludzkimi.

Metoda szkolenia:

Szkolenie prowadzone jest metodą wykładowo - warsztatowo - prezentacyjną, z aktywnym uczestnictwem słuchaczy w dyskusjach w wybranych tematach

Zakres szkolenia:

Moduł 1: Informacja jako ważny aktyw każdej Firmy

- Nowa, rozszerzona definicja informacji we współczesnym świecie
- Podstawy prawne ochrony aktywów przedsiębiorstwa
- Pojęcie wielowątkowego Bezpieczeństwa Informacji
- Zasadność kompleksowego podejścia do wdrożenia zasad bezpieczeństwa.
- Nowe sposoby ochrony dla pracowników: świadome zachowania pro-bezpieczne
- Najciekawsze przykłady zaczerpnięte ze światowej i polskiej literatury, opisywane m.in. przez najbardziej znanych na świecie hackerów.
- Sposoby selekcji i klasyfikacji aktywów informacyjnych
- Dyskusja uczestników szkolenia, odnosząca się do konkretnych warunków i rodzajów informacji w ich Firmie.

Business People Alignment



Moduł 2: Rodzaje zagrożeń oraz sposoby ochrony i przeciwdziałania

- Klasyfikacja zagrożeń. Uczestnicy są zapoznawani z najważniejszymi rodzajami zagrożeń w dziedzinie ochrony i bezpieczeństwa informacji
- Incydenty bezpieczeństwa - skutki bezpośrednie i pośrednie
- Czy nasze urządzenia wielofunkcyjne, nasza centrala telefoniczna są dla nas zagrożeniem? Wytyczne i zalecenia.
- Tradycyjny a nowoczesny nabór pracowników: zagrożenie czy szansa?
- Metody i reguły perfidnego oddziaływania socjotechników na naszych pracowników oraz praktyczne sposoby obrony i ochrony przed nimi
- Przykładowa wielostopniowa procedura weryfikacji intruza

Moduł 3: Internet, poczta elektroniczna, systemy zabezpieczeń

- Poczta elektroniczna – zagrożenia i praktyczne metody ochrony przydatne dla każdego pracownika
- Internet - zagrożenia i praktyczne metody ochrony przydatne dla każdego pracownika
- Systemy zabezpieczeń, cele stosowania, przykłady wdrożeń
- Wytyczne: jak stworzyć dobre i „trudne” hasło oraz: jak je chronić?
- Techniki inwigilacji – opis możliwości oraz jak sobie z nimi radzić?

Moduł 4: Odniesienia do normy PN-ISO/IEC 27001:2007

- Budowa Kompleksowej Polityki Bezpieczeństwa Firmy
- Kluczowa rola tzw. „czynnika ludzkiego”
- Jaki wpływ ma Kierownictwo firmy na postawy pracowników wobec ochrony wrażliwych aktywów swojej firmy ?
- Audyt Bezpieczeństwa Firmy wg normy PN-ISO/IEC 27001:2007
- Jakie elementy normy można wprowadzać w życie na bazie tego szkolenia?
- Przestępstwa wirtualne – jak się bronić?
- Podsumowanie treści szkolenia

Czas trwania – 1 dzień, (ok. 5 godzin)

Business People Alignment

