I know IT by softinet

KNOWLEDGE THAT
EMPOWERS BUSINESS

Security Awareness - Świadoma i bezpieczna Organizacja

Korzystając z naszego wykładu dowiesz się:

- jak połączyć biznes z cyberbezpieczeństwem
- jakie są zagrożenia i potencjalne straty biznesowe
- czym jest i jak zbudować politykę bezpieczeństwa korporacyjnego
- jak podnieść świadomości pracowników o realnych zagrożeniach w cyberprzestrzeni

Czas
1 DZIEŃ

Godziny
9:00 - 13:00

Certyfikat
TAK

OPIS SZKOLENIA

Pracownik odgrywa bardzo istotną rolę w zakresie bezpieczeństwa całej organizacji. Jest on ostatnią linią obrony przed zagrożeniami w cyberprzestrzeni, a jednocześnie podatny na działania socjotechniczne z dostępem bezpośrednim do systemów i danych wrażliwych. Okazuje się, że to pracownicy są najczęściej na celowniku przestępców, dlatego tak bardzo ważne jest budowanie ich świadomości o potencjalnych zagrożeniach w Internecie. Dzięki temu szkoleniu dowiesz się m. in. czym jest socjotechnika i jak jest wykorzystywana przez przestępców, czym są zagrożenia zewnętrzne i wewnętrzne w organizacji. Dowiesz czym jest audyt i polityka bezpieczeństwa korporacyjnego, jak przetwarzać dane w systemach oraz inne zagadnienia „nieinformatyczne" wpływające pośrednio i bezpośrednio na bezpieczeństwo organizacji. Zdobędziesz wiedzę jak z poziomu maganementu budować świadomość u pracowników na temat cyberbezpieczeństwa oraz jak racjonalnie budować kompetencje IT.

CEL SZKOLENIA

Uczestnicy dowiedzą się w jaki sposób racjonalnie zarządzać obszarem IT aby budować bezpieczną organizację. Podczas wykładu bardzo duży nacisk położony jest na biznesową korelację z bezpieczeństwem IT.

FORMA SZKOLENIA

Szkolenie prowadzone jest w formie wykładów.

WYMAGANIA

Wykład przeznaczony jest dla kadry zarządzającej.

Security Awareness - Świadoma i bezpieczna Organizacja

Agenda szkolenia:

Wprowadzenie
Zagrożenia - modus operandi
zagrożenia zewnętrzne – maile, www, social media,
zagrożenia zewnętrzne – Fake News'y
zagrożenia wewnętrzne - pracownik
zagrożenia wewnętrzne - praca zdalna
zagrożenia wewnętrzne – cyberterroryzm

Potencjalne straty biznesowe
wizerunkowe
finansowe

Dostęp i przetwarzanie danych
klasyfikacja danych
zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem
dostęp do danych
wyciek danych – naruszenie bezpieczeństwa danych
bezpieczne przetwarzanie danych
polityka czystego biurka

Analiza ryzyka
jak i w jakim celu wykonywana jest analizę ryzyka
macierz ryzyka
zarządzanie ryzykiem
BCMS - plany awaryjne, odtworzeniowe

Audyt systemu informatycznego
czym jest i co powinien zawierać audyt

Polityka bezpieczeństwa korporacyjnego
czym jest i jak zdefiniować firmową politykę bezpieczeństwa
przykład Polityki Bezpieczeństwa korporacyjnego

Narzędzia do zabezpieczeń/nadzoru/monitorowania
przykładowe narzędzia wspomagające cyberbezpieczeństwo firmy

Best Practice
Przykłady rozwiązań/wdrożeń

TRENER - Michał Cygan

Inżynier **FORTINET** posiadający doświadczenie w zakresie wdrażania i wsparcia omawianych rozwiązań.

www.iknowit.com.pl

AL. JEROZOLIMSKIE 142B, 02-305 WARSZAWA

szkolenia@ iknowit.com.pl

(22) 427 37 54 / +48 728 540 162