POLSKIE CENTRUM
BADAŃ I CERTYFIKACJI

SZKOLENIE

Bezpieczny pracownik w sieci z elementami anty-inwigilacji

1 DZIEŃ **8 GODZIN LEKCYJNYCH**

ONLINE **SYMBOL: O235**

Termin zgodnie z harmonogramem szkoleń otwartych PCBC S.A. dostępnym na stronie: www.pcbc.gov.pl

DLACZEGO MY?

- Szeroki wybór tematów
- Realizacja celu
- Najlepsi trenerzy
- 60 lat na rynku
- Atrakcyjna forma

Polskie Centrum Badań i Certyfikacji S.A.
ul. Puławska 469
02-844 Warszawa
Tel.: +48 22 46 45 200
pcbc@pcbc.gov.pl

O SZKOLENIU

Szkolenie, którego celem jest zwiększenie bezpieczeństwa organizacji i osób prywatnych poprzez podnoszenie kompetencji pracowników w zakresie bezpieczeństwa IT, w szczególności w zakresie ochrony danych, informacji i wiedzy na temat zagrożeń sieciowych, inżynierii społecznej oraz programowych i fizycznych podsłuchów. Szkolenie ma za zadanie nauczyć pracowników jak korzystać z urządzeń IOT - komputera, smartfonu i innych urządzeń teleinformatycznych, tak aby nie narażać prywatnych danych czy danych firmy na ataki cyberprzestępców. Dodatkowo, nasze rozszerzone szkolenie rzuca światło na techniki wykorzystywane przez cyberprzestępców w celu inwigilacji, zarówno przy użyciu podsłuchów programowych, jak i fizycznych.

PROGRAM SZKOLENIA

- Zagrożenia w cyberprzestrzeni dla pracownika oraz dla zasobów organizacji – obecne trendy.
- Socjotechniczne mechanizmy działania cyberprzestępców w domu i w firmie.
- Dobre praktyki zabezpieczania się przed poszczególnymi zagrożeniami, w tym budowania skutecznych haseł, tworzenia kopii bezpieczeństwa.
- Rozpoznawanie złośliwego oprogramowania i innych ataków na firmę oraz reagowanie na pojawiające się niebezpieczeństwa.
- Krótkie omówienie obowiązku ochrony informacji i zabezpieczania środowiska pracy z podkreśleniem indywidualnej odpowiedzialności za utrzymanie bezpieczeństwa informacji i reputacji instytucji oraz zaufania klientów.
- Przykładowe narzędzia pomocne w obronie przed atakami w sieci.
- Przenoszenie się zagrożeń pomiędzy obszarem prywatnym a służbowym.
- Profilaktyka bezpiecznego korzystania z Internetu oraz sieci LAN/WIFI.
- Bezpieczeństwo urządzeń IOT (Internet of Thinks).
- Pokaz przykładowych ataków:
  - atak MITM: podsłuch i modyfikacja wiadomości pomiędzy dwiema stronami,
  - kradzież haseł,
  - podmiana stron internetowych.
- Pokaz wybranych ataków wykonywanych przez cyberprzestępców na smartfony.
- Ochrona urządzeń mobilnych przed hakerami – oprogramowanie szpiegujące.
- Omówienie technik inwigilacji elektronicznej:
  - zrozumienie zagrożeń związanych z podsłuchem i inwigilacją.
- Omówienie technik ochrony przed podsłuchem i inwigilacją elektroniczną:
  - sposoby ochrony przed podsłuchem (np. szyfrowanie komunikacji, korzystanie z aplikacji do bezpiecznych rozmów, rekomendowane autorskie sposoby).

KORZYŚCI

- Wzrost bezpieczeństwa IT, organizacja będzie bardziej odporna na ataki cybernetyczne, co przekłada się na zwiększone ogólne bezpieczeństwo.
- Skuteczniejsza reakcja na incydenty: pracownicy będą lepiej przygotowani do rozpoznawania i reagowania na potencjalne zagrożenia, co może ograniczyć skutki ewentualnych incydentów.
- Szkolenie pomaga zrozumieć znaczenie bezpieczeństwa IT i jakie są potencjalne konsekwencje naruszenia bezpieczeństwa, co przyczynia się do większej uwagi i zaangażowania w tym obszarze.
- Szkolenie zapozna się z metodami inwigilacji poprzez podsłuchy fizyczne i programowe oraz pozwoli na wdrożenie technik anty-inwigilacyjnych.

1200 ZŁ

NETTO / OSOBA

Cena obejmuje: organizację szkolenia w trybie on-line,
materiały szkoleniowe w formie elektronicznej,
certyfikat uczestnictwa w formie papierowej.

CERTYFIKACJA. BADANIA. SZKOLENIA.

Więcej informacji

Agnieszka Korczak
Kom.+48 691 192 671
email: akorczak@pcbc.gov.pl

Mariola Fijewska
Kom.+48 665 464 661
email:mfijewska@pcbc.gov.pl

Natalia Nowak
Kom.+48 669 474 742
email: nowak@pcbc.gov.pl