Projekt „Naprzeciw oczekiwaniom - akademia kompetencji językowych i komputerowych" jest współfinansowany ze środków Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2014-2020

„Akademia kompetencji IT PRO – Cyberbezpieczeństwo"

Program szkolenia:

1. Moduł nr 0. Powszechność zagrożeń cyberprzestępczości
   - Jak powszechne są cyberprzestępstwa – statystyki
   - Kim jest cyberprzestępca?
   - Socjotechnika i manipulacje
   - Na jakich emocjach działają oszuści
   - Przykłady ogłoszeń w darknecie
   - Czym ryzykujemy zaniedbując cyberbezpieczeństwo?
2. Moduł nr 1. Człowiek jako najsłabsze ogniwo
   - Przykładowe ataki z pominięciem narzędzi cyberbezpieczeństwa
   - Dlaczego najsłabszym ogniwem jest człowiek
   - Kogo wybiera cyberprzestępca
3. Moduł nr 2. – System cyberbezpieczeństwa
   - Podstawowe narzędzia cyberbezpieczeństwa
   - Z czego powinien składać się skuteczny system cyberbezpieczeństwa
   - Jak go zbudować?
4. Moduł nr 3. Najpowszechniejsze zagrożenia w sieci
   - Rodzaje zagrożeń sieciowych
   - Wirusy
   - Koń trojański i bomba logiczna
   - Exploity
   - Robaki
   - Rokity
   - Spyware
   - Inne zagrożenia w sieci
5. Moduł nr 4. Zagrożenia sieciowe jak się bronić?
   - Skąd się bierze złośliwe oprogramowanie – przykłady
   - Jak je rozpoznać?
   - Jak je usuwać?
   - Jak się bronić przed złośliwym oprogramowaniem
6. Moduł nr 5. Bezpieczna praca w firmie
   - Rodzaje zagrożeń w codziennej pracy w firmie
   - Zasady czystego biurka
   - Zasady czystego ekranu
   - Co należy szczególnie chronić

Biuro Projektu: RECON Consulting Sp. z o.o.
ul. Armii Krajowej 81/3, 41-506 Chorzów
tel.: 531-238-712 lub 570-506-561,
e-mail: akademia@rcon.com.pl
www.akademia-szkolen.pl

- Procedury bezpiecznej pracy

7. Moduł nr 6. Podejrzane urządzenia elektroniczne
   - Zagrożenia urządzeń elektronicznych
   - Przykłady zagrożeń laptopy, pendrive, smartfony
   - Jak się przed tym chronić?
8. Moduł nr 7. Zagrożenia sieci WiFi
   - Publiczne i nie sprawdzone hotspoty – zagrożenia
   - Case study – przykładowych zagrożeń
   - Bezpieczna praca z WiFi
   - Konfiguracja segmentacji sieci
9. Moduł nr 8. Ransomware
   - Ransomware jako najczęstszy rodzaj ataków na firmy i instytucje
   - Przykłady ataków i konsekwencji
   - Jak się chronić i na co zwracać uwagę
10. Moduł nr 9. Spyware i Keylogger
    - Rodzaje zagrożeń związanych z keylogger i spyware
    - Przykłady ataków – utrata danych, podmiany kont bankowych
    - Skąd je mamy?
    - Jak się przez tym bronić?
11. Moduł nr 10. Niebezpieczeństwo aplikacji
    - Jakie aplikacje są niebezpieczne
    - Zagrożenia związane z niebezpiecznymi aplikacjami
    - Jak się bronić i na co zwracać uwagę
12. Moduł nr 11. Niebezpieczeństwo komunikatorów i social mediów
    - Jak podszyć się pod kogoś w social mediach
    - Niebezpieczeństwo komunikatorach i social mediach
    - Przykłady ataków
    - Jak się przed tym bronić?
13. Moduł nr 12. Bezpieczna praca z pocztą elektroniczną
    - Zagrożenia związane z pocztą elektroniczną
    - Przykłady fałszywych e-maili
    - Jak pracować bezpiecznie z poczta elektroniczną?
14. Moduł nr 13. Phishing jak się nie dać złowić, na co zwracać uwagę
    - Phishing – czym jest, jak działa?
    - Przykłady zagrożeń związanych z Phishingem
    - Jak zidentyfikować Phishing?
    - Jak się bronić przed Phishingiem?
    - Phishing Quiz
    - Praca z symulatorem ataków

15. Moduł nr 14. Bezpieczeństwo haseł
   - Skąd cyberprzestępcy mają nasz hasła?
   - Jak zweryfikować możliwość utraty haseł?
   - Jak bezpiecznie tworzyć i organizować hasła – przykładowe narzędzia
   - Jak zapewnić 99,99% bezpieczeństwo dla swoich dostępów
   - Konfiguracja menadżera haseł
16. Moduł nr 15. Bezpieczeństwo pracy zdalnej
   - Zagrożenia w pracy zdalnej
   - Przykłady możliwych ataków
   - Bezpieczeństwo danych
   - Jak bezpiecznie pracować na odległość – podstawowe zasady
   - VPN – instalacja i konfiguracja
17. Moduł nr 16. Ochrona Danych Osobowych
   - Podstawy ochrony danych osobowych
   - Akty prawne regulujące ochronę danych osobowych
   - Administratora o podmiot przetwarzający
   - Obowiązki informacyjne
   - Zgody na przetwarzania danych
   - Powierzenia przetwarzania danych
   - Upoważnienia do przetwarzania danych
18. Moduł nr 17. System zarządzania bezpieczeństwem informacji w oparciu o normy ISO 27001 / ISO 27002
   - omówienie wymagań normy ISO 27001
   - metoda analizy ryzyka bezpieczeństwa informacji
   - deklaracja stosowania, w tym polityki bezpieczeństwa
   - podręcznik bezpieczeństwa informacji
   - metoda analizy ryzyka bezpieczeństwa informacji
   - planowanie ciągłości działania
   - klasyfikacja informacji
   - nadawanie, zmiany uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemach informatycznych
   - zarządzanie bezpieczeństwem fizycznym i dostępem do pomieszczeń
   - zarządzanie bezpieczeństwem fizycznym sprzętu i nośników
   - użytkowanie stanowiska komputerowego
   - zarządzanie incydentami
   - procedura zarządzania zamianami
   - ochrona danych osobowych
   - procedura implementacji i wycofania systemów teleinformatycznych
   - procedura zarządzania dostępem do sieci i systemów
   - procedura organizacja środków ochrony fizycznej

19. Moduł nr 18. Zabezpieczenia systemowe wg. załącznika A do normy ISO 27001
   - Omówienie załącznika A do normy ISO 27001
   - Wskazanie praktycznych rozwiązań i zabezpieczeń wynikających z załącznika A do normy ISO 27001
20. Moduł nr 19. Audyt i rozwój systemów bezpieczeństwa informacji
   - Zarządzanie programem audytów ISO 27001
   - Odpowiedzialność auditora
   - Cechy osobiste auditora
   - Kompetencje auditora
   - Oparte na ryzyku podejście do zasad audytu
   - Ukierunkowanie na proces
   - Wykonalność audytu ISO 27001
   - Dokumenty niezbędne auditorowi do tego, aby przeprowadzić audyt w sposób właściwy (plan, listy kontrolne)
   - Przeprowadzenie spotkania otwierającego
   - Dokumentowanie działań audytowych
   - Dowody z audytu i ich ocena
   - Formułowanie niezgodności oraz potencjałów do doskonalenia
   - Formułowanie wniosków
   - Przeprowadzenie spotkania zamykającego audyt
   - Tworzenie raportu z audytu
   - Dobre praktyki audytowe
21. Moduł 20 - Podstawy zabezpieczania sieci - systemy Firewall
   - typy Fireawalli
   - konfiguracja Firewalla
   - ustalanie zestawu reguł Firewalla
   - systemy UTM
22. Moduł 21 - Konfiguracja urządzeń sieciowych pod katem monitorowania i analizy ruchu Systemy
   - wykrywania włamań
   - IDS hostowy
   - IDS sieciowy określanie zasad monitorowania zdarzeń
   - reakcje na incydent
   - HoneyPot - „garnek miodu" typy honeypotów instalacja i konfiguracja
   - Zarządzanie logami
   - logi systemowe
   - logi z systemów bezpieczeństwa
   - strategia archiwizacji logów