ZAKŁAD ROZWOJU TECHNICZNEJ OCHRONY MIENIA TECHOM SP. Z O.O.

Jednostka Certyfikująca
na Znak PN
PN-EN 16763

Al. Wyzwolenia 12, 00-570 Warszawa
tel. (22) 625-34-00, fax (22) 625-26-75
www.techom.com
techom@techom.com

Wpis do KRS Nr 0000164572
NIP: 5260011894
Regon: 010663796

KOD NCAGE **9A57H**

SZKOLENIE:

CYBERBEZPIECZEŃSTWO W SYSTEMACH ZABEZPIECZEŃ TECHNICZNYCH

przeznaczone dla osób pełniących / przygotowywanych do pełnienia funkcji m.in.:

- projektantów, instalatorów, konserwatorów i administratorów systemów zabezpieczeń technicznych – pracowników zabezpieczenia technicznego
- koordynatorów projektów systemów zabezpieczenia technicznego
- osób zarządzających bezpieczeństwem obiektów
- menedżerów, specjalistów, konsultantów ds. cyberbezpieczeństwa, zarzadzania bezpieczeństwem informacji
- osób zajmujących się ochroną infrastruktury krytycznej
- pracowników operatorów usług kluczowych oraz dostawców usług cyfrowych odpowiedzialnych za wdrożenia systemu zarzadzania bezpieczeństwem
- prawników obsługujących projekty dot. cyberbezpieczeństwa
- administratorów sieci
- szefów sekcji ochrony obiektów, administratorów systemów alarmowych, komendantów ochrony, osób nadzorujących i użytkujących systemy zabezpieczeń w jednostkach wojskowych

EFEKTY UCZENIA:

Udział w kursie pozwala na uzyskanie niezbędnej, specyficznej wiedzy dot. bezpieczeństwa cybernetycznego systemów zabezpieczeń technicznych. Absolwent kursu m.in:

1. Charakteryzuje pojęcia z zakresu cyberbezpieczeństwa z naciskiem na obszar systemów zabezpieczeń technicznych
2. Zna i posługuje się podstawowymi i niezbędnymi wymaganiami dotyczącymi ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w odniesieniu do organizacji według rodziny norm ISO/IEC 27000
3. Zna i posługuje się podstawowymi i niezbędnymi wymaganiami dotyczącymi szacowania ryzyka dla systemów zabezpieczeń technicznych
4. Identyfikuje i grupuje wartości aktywów
5. Kategoryzuje zagrożenia i podatności (ryzyka) aktywów
6. Identyfikuje i wartościuje zagrożenia oraz ataki, a także techniki wykorzystywania słabości bezpieczeństwa;
7. Dobiera i uzasadnia metody zapewnienia usystematyzowanego podejścia do zarządzania i obsługi incydentów bezpieczeństwa informacji;
8. Omawia zasady klasyfikacji i kwalifikacji zdarzeń jako incydentów bezpieczeństwa;
9. Charakteryzuje współczesne rozwiązania bezpieczeństwa sieciowego dla systemów zabezpieczeń technicznych
10. Charakteryzuje rodzaje testów penetracyjnych

Szkolenie trwa 3 dni.

Wartość:

- **FORMA ZDALNA – MS TEAMS:** jedna osoba - **2650,00 zł netto** (słownie: dwa tysiące sześćset pięćdziesiąt złotych)

Do podanych powyżej cen należy doliczyć 23% VAT, niemniej szkolenia w zakresie kształcenia zawodowego lub przekwalifikowania zawodowego finansowane w co najmniej 70% ze środków publicznych są zwolnione z VAT – instytucje, które spełniają ten wymóg prosimy o przesłanie stosownego oświadczenia wraz ze zgłoszeniem uczestnictwa.

Koszty udziału obejmują: szkolenie, materiały dydaktyczne, wydanie zaświadczenia o ukończeniu szkolenia.

Szkolenie kończy się wydaniem bezterminowego zaświadczenia o ukończeniu szkolenia.

Zgłoszenia:

Celem zgłoszenia należy odesłać skan podpisanej karty zgłoszenia na mail: techom@techom.com oraz potwierdzenia wykonania przelewu. Uwaga: jednostki finansowane z budżetu państwa lub spółki skarbu państwa dokonują opłat po odbyciu szkolenia.

Poza przesłaniem maila należy skontaktować się z Zakładem TECHOM telefonicznie i potwierdzić zgłoszenie: 22-625-34-00.

WSTĘPNY - RAMOWY PROGRAM SZKOLENIA

UWAGA: program szkolenia będzie dostosowany do projektowanych przepisów prawa implementujących Dyrektywę NIS2

Moduł 0: Wstęp do Cyberbezpieczeństwa

1. Definicje i podstawowe pojęcia
   - Co to jest cyberbezpieczeństwo?
   - Kluczowe terminy: zagrożenia, podatności, ataki, ochrona.
2. Znaczenie cyberbezpieczeństwa w systemach bezpieczeństwa fizycznego
   - Przegląd systemów: CCTV, kontrola dostępu, systemy alarmowe.
   - Potencjalne zagrożenia i ich konsekwencje.

Moduł 1: Kontekst prawno-normatywny

1. Ustawa o Krajowym Systemie Cyberbezpieczeństwa
   - Zakres podmiotowy
   - Obowiązki operatorów usług kluczowych
   - Wymagania wobec dostawców usług dla podmiotów ważnych, kluczowych i krytycznych w swietle przepisów implementujących NIS2
2. Ustawa o zarządzaniu kryzysowym
   - Infrastruktura Krytyczna
3. Wyzwania compliance w cyberbezpieczeństwie
4. Normy, standardy i wymagania branżowe
5. Ochrona danych osobowych
6. Uprawnienia audytorów systemów zabezpieczeń technicznych

Moduł 2: Proces wdrażania cyberbezpieczeństwa w organizacji

1. Inwentaryzacja zasobów
2. Mapowanie procesów
3. Audyty zgodności
4. Ocena ryzyka i ocena skutków
5. Tworzenie dokumentacji – polityki i instrukcje
6. Szkolenia pracowników
7. Wdrożenie procedur i rekomendacji
8. Audyty powdrożeniowe

Moduł 3: Podstawy Cyberbezpieczeństwa

1. Podstawowe zagrożenia i ataki
   - Malware, ransomware, phishing, ataki DDoS.
2. Podstawowe mechanizmy ochrony
   - Firewalle, antywirusy, systemy wykrywania intruzów (IDS/IPS).
3. Bezpieczeństwo sieciowe
   - Zasady segmentacji sieci.
   - Bezpieczna konfiguracja routerów i switchy.
4. Podstawy kryptografii
   - Szyfrowanie danych, klucze kryptograficzne, certyfikaty.

Moduł 4: Bezpieczeństwo sprzętu sieciowego i urządzeń

1. Podstawowa wiedza o sieciach i zasady bezpieczeństwa informacji
2. Bezpieczeństwo komunikacji sieciowej
3. Instalacja i konfiguracja
4. Zapewnienie jakości oprogramowania i bezpieczeństwo
5. Standardy operacyjne, polityki i oceny ryzyka

Moduł 5: Architektura systemów bezpieczeństwa fizycznego

1. Bezpieczeństwo CCTV
    - Architektura systemów CCTV
    - Podatności i zagrożenia w systemach CCTV
    - Metody zabezpieczania systemów CCTV
2. Bezpieczeństwo systemów kontroli dostępu
    - Architektura systemów kontroli dostępu
    - Podatności i zagrożenia w systemach kontroli dostępu
    - Metody zabezpieczania systemów kontroli dostępu
3. Bezpieczeństwo systemów alarmowych
    - Architektura systemów alarmowych
    - Podatności i zagrożenia w systemach alarmowych
    - Metody zabezpieczania systemów alarmowych

Moduł 6: Rola projektanta systemów bezpieczeństwa

1. Poznanie roli projektanta systemów bezpieczeństwa
2. Relacje między konsultantami a integratorami
3. Identyfikacja elementów dokumentacji odpowiedzialnych za cyberbezpieczeństwo
4. Ważne funkcje i symbole w dokumentacji projektowej

Moduł 7: Bezpieczeństwo IT i infrastruktura

1. Opis podstawowej infrastruktury IT
2. Przegląd wymagań dotyczących konserwacji systemów operacyjnych i firmware
3. Klasyfikacja zagrożeń dla bezpieczeństwa informacji systemów sieciowych
4. Identyfikacja powszechnych luk w zabezpieczeniach systemów sieciowych

Moduł 8: Incydenty

1. Rodzaje incydentów
2. Zgłaszanie incydentów
3. Obsługa incydentów wewnątrz organizacji
4. Wnioski i dalsze postępowanie w tym analiza powłamaniowa

Moduł 9: Bezpieczeństwo cybernetyczne - jaki mamy problem?

1. Realia doby komunikacji globalnej
2. Urządzenia i technologie "smart"
3. Urządzenia IoT (Internet of Things)
4. Główne podmioty w sferze bezpieczeństwa cybernetycznego
5. Case study - przykłady naruszeń bezpieczeństwa cybernetycznego
6. Ryzyko a zagrożenie w kontekście bezpieczeństwa cybernetycznego

Moduł 10: Problem bezpieczeństwa cybernetycznego "od kuchni"

1. Czynnik ludzki
2. Architektura współczesnych systemów zabezpieczeń technicznych
3. Inżynieria oprogramowania i błędy jako jeden z jej elementów
4. Podstawowe zasady bezpieczeństwa
5. Bezpieczeństwo fizyczne
6. Bezpieczeństwo komputerów i urządzeń mobilnych

Moduł 11: Hacking

1. Jak to się zaczęło
2. Co to jest hacking
3. Najczęściej stosowane techniki ataków cybernetycznych
4. Podatność i backdoor
5. Ataki Socjotechniczne (inżynieria społeczna)
6. Złośliwe oprogramowanie

Moduł 12: ISO27001 jako narzędzie w zarządzaniu bezpieczeństwem

1. Zarys normy PN-EN ISO/IEC 27001: 2023-08
2. Cykl Deminga i System Zarządzania Bezpieczeństwem Informacji
3. Przykłady praktycznej implementacji PN-EN ISO/IEC 27001 w systemach zabezpieczeń technicznych
4. Aspekt audytowania systemów zabezpieczeń technicznych

Moduł 13: Podatności na zagrożenia

1. Kluczowe cechy spójnego i skutecznego systemu informatycznego
2. Podatności w systemach zabezpieczeń technicznych
3. Zarządzanie podatnościami jako element polityki bezpieczeństwa
4. Wyszukiwanie podatności
5. Celowe i niepożądane ujawnianie podatności
6. Zarządzanie aktualizacjami produktów

Moduł 14: Publiczne bazy podatności

Moduł 15: Badanie bezpieczeństwa

1. Obszary badań sprzętu i oprogramowania
2. Testy penetracyjne
3. Przykładowe narzędzia do badania bezpieczeństwa cybernetycznego

Moduł 16: Bezpieczeństwo cybernetyczne w praktyce - demonstracje

1. Atak typu "bruteforce" - Demonstracja włamania do systemu informatycznego metodą "brutalnego" łamania hasła logowania

2. Atak typu "middleman" na niezabezpieczonym protokole HTTP - Demonstracja podsłuchiwania transmisji danych i ich modyfikacji w czasie rzeczywistym między komputerami serwera i klienta (fabrykacja danych)
3. Oszustwo "na znaki specjalne" w nazwach domenowych - Stworzenie fałszywej domeny, "udającej" oryginalną stronę, np. banku i próba wyłudzenia danych logowania (kradzież tożsamości klienta)
4. Podgląd nieszyfrowanego strumienia wizyjnego - Demonstracja nieautoryzowanego uzyskania dostępu do obrazu z kamery CCTV (podgląd obrazu bez logowania)
5. Filtracja adresów - biała i czarna lista w praktyce - Demonstracja działania technik blokowania ruchu w sieci IP na podstawie adresów MAC lub IP (blokowanie transmisji)
6. Sieci bezprzewodowe - przykładowe podatności - Demonstracja śledzenia aktywności i lokalizacji komputera na podstawie analizy danych z sieci WiFi oraz wykorzystanie tych danych do infiltracji sieci podmiotów gospodarczych
7. Różne przykłady praktycznych zabezpieczeń w sprzęcie i oprogramowaniu - Demonstracje różnych technik ochrony danych i transmisji w sprzęcie i oprogramowaniu komputerowym

Moduł 17: Bezpieczeństwo sieci

1. Narażenia protokołów modelu ISO/OSI
2. Segmentacja i separacja sieci
3. Sieci VLAN
4. Filtracja adresów MAC i IP
5. Bezpieczeństwo routingu

Moduł 18: Systemy chmurowe

1. Wyzwania otoczenia chmurowego
2. Modele usług chmurowych
3. Modele wdrożeniowe

Moduł 19: Bezpieczeństwo produktów i danych

1. Sprzęt i oprogramowanie
2. Dane
3. Zarządzanie bezpieczeństwem w inżynierii oprogramowania

Moduł 20: Podstawy zarządzania ryzykiem dla systemów zabezpieczeń w odniesieniu do międzynarodowych standardów

1. Akty prawne
2. Analiza Ryzyka
3. Szacowanie Ryzyka
4. Aktywa i Zasoby
5. Zagrożenia i Podatności

Moduł 21: Architektura cyberbezpieczeństwa systemów zabezpieczeń technicznych. Secure by design i secure by default.

Moduł 22: Planowanie, projektowanie i instalowanie cyberbezpiecznych systemów zabezpieczeń technicznych.

Moduł 23: Wytyczne TECHOM w zakresie cyberbezpieczeństwa systemów zabezpieczeń technicznych. Dobre praktyki. Podsumowanie i wnioski

1. Podsumowanie najważniejszych zagadnień
2. Najlepsze praktyki w zakresie cyberbezpieczeństwa systemów zabezpieczeń technicznych
3. Q&A oraz sesja dyskusyjna

Wykładowcami będą znani i cenieni specjaliści ds. cyberbezpieczeństwa, w tym byli i obecni kierownicy komórek odpowiedzianych za cyberbezpieczeństwo w administracji rządowej i/lub instytucjach infrastruktury krytycznej, specjaliści ds. bezpieczeństwa sieci, specjaliści w zakresie testów penetracyjnych i rzeczoznawcy ds. systemów zabezpieczeń technicznych.

Organizator szkolenia zastrzega sobie prawo do zmian w planie szkolenia zgodnie z występującymi potrzebami w tym zakresie. Ostateczny plan szkolenia uczestnicy otrzymają w pierwszym dniu szkolenia, przed jego rozpoczęciem. Organizator zastrzega również prawo do zmiany planu szkolenia w trakcie jego trwania.