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 I SYSTEMACH OCHRONY PRZECIWPOŻAROWEJ

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 2 dni.

Wartość:

- **FORMA STACJONARNA BEZ ZAKWATEROWANIA:** jedna osoba - **1950,00 zł netto** (słownie: jeden tysiąc dziewięćset pięćdziesiąt złotych)
- **FORMA STACJONARNA Z ZAKWATEROWANIEM OD 28.06:** jedna osoba - **2400,00 zł netto** (słownie: dwa tysiące czterysta złotych) – pokój 1 os.
- **FORMA STACJONARNA Z ZAKWATEROWANIEM OD 29.06:** jedna osoba - **2200,00 zł netto** (słownie: dwa tysiące dwieście złotych) – pokój 1 os.

Miejsce szkolenia: Warszawa

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, całodzienny bufet kawowy, wyżywienie w ramach szkolenia, opcjonalnie - zakwaterowanie

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.

PROGRAM SZKOLENIA

Dzień I szkolenia CYBER

L.p.	Dzień szkolenia	Godz. od - do	Czas trwania [min]	Temat wykładu/ćwiczeń
1.	29.06.2022	9.00 – 9.30	30	Bezpieczeństwo cybernetyczne - jaki mamy problem? • Realia doby komunikacji globalnej • Urządzenia i technologie "smart" • Główne podmioty w sferze bezpieczeństwa cybernetycznego • Case study - przykłady naruszeń bezpieczeństwa cybernetycznego • Ryzyko a zagrożenie w kontekście bezpieczeństwa cybernetycznego
2.		9.30 – 10.00	30	Problem bezpieczeństwa cybernetycznego "od kuchni" • Czynnik ludzki • Architektura współczesnych systemów zabezpieczeń technicznych • Inżynieria oprogramowania i błędy jako jeden z jej elementów
3.		10.00 – 10.10	10	PRZERWA KAWOWA
4.		10.10 – 11.10	60	Hacking • Jak to się zaczęło • Co to jest hacking • Najczęściej stosowane techniki ataków cybernetycznych • Podatność i backdoor
5.		11.10 – 11.15	5	PRZERWA KAWOWA
6.		11.15 – 11.45	30	ISO27001 jako narzędzie w zarządzaniu bezpieczeństwem • Zarys normy PN-ISO/IEC 27001:2017-06 • Cykl Deminga i System Zarządzania Bezpieczeństwem Informacji • Przykłady praktycznej implementacji ISO-27001 w systemach zabezpieczeń technicznych
7.		11.45 – 12.45	60	Podatności na zagrożenia • Kluczowe cechy spójnego i skutecznego systemu informatycznego

L.p.	Dzień szkolenia	Godz. od - do	Czas trwania [min]	Temat wykładu/ćwiczeń
				• Podatności w systemach zabezpieczeń technicznych • Zarządzanie podatnościami jako element polityki bezpieczeństwa • Wyszukiwanie podatności • Celowe i niepożądane ujawnianie podatności • Zarządzanie aktualizacjami produktów Publiczne bazy podatności
8.		12.45 – 13.45	60	PRZERWA OBIADOWA
9.		13.45 – 14.45	60	Badanie bezpieczeństwa • Obszary badań sprzętu i oprogramowania • Testy penetracyjne • Przykładowe narzędzia do badania bezpieczeństwa cybernetycznego
10.		14.45 – 15.00	15	PRZERWA KAWOWA
11.		15.00 – 16.00	60	Bezpieczeństwo cybernetyczne w praktyce - demonstracje • Atak typu "brute force" - Demonstracja włamania do systemu informatycznego metodą "brutalnego" łamania hasła logowania • Atak typu "middle man" na niezabezpieczonym protokole HTTP - Demonstracja podsłuchiwania transmisji danych i ich modyfikacji w czasie rzeczywistym między komputerami serwera i klienta (fabrykacja danych) • Oszustwo "na znaki specjalne" w nazwach domenowych - Stworzenie fałszywej domeny, "udającej" oryginalną stronę, np. banku i próba wyłudzenia danych logowania (kradzież tożsamości klienta) • Podgląd nieszyfrowanego strumienia wizyjnego - Demonstracja nieautoryzowanego uzyskania dostępu do obrazu z kamery CCTV (podgląd obrazu bez logowania) • Filtracja adresów - biała i czarna lista w praktyce - Demonstracja działania technik blokowania ruchu w sieci IP na podstawie adresów MAC lub IP (blokowanie transmisji) • 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 • Różne przykłady praktycznych zabezpieczeń w sprzęcie i oprogramowaniu - Demonstracje różnych technik ochrony danych i transmisji w sprzęcie i oprogramowaniu komputerowym

Dzień II szkolenia CYBER

L.p.	Dzień szkolenia	Godz. od - do	Czas trwania [min]	Temat wykładu/ćwiczeń
1.	30.06.2022	9.00 – 10.00	60	Bezpieczeństwo sieci • Narażenia protokołów modelu ISO/OSI • Segmentacja i separacja sieci • Sieci VLAN • Filtracja adresów MAC i IP • Bezpieczeństwo routingu Systemy chmurowe
2.		10.00 – 10.10	10	PRZERWA KAWOWA
3.		10.10 – 11.10	60	Bezpieczeństwo produktów i danych • Sprzęt i oprogramowanie • Dane • Zarządzanie bezpieczeństwem w inżynierii oprogramowania
4.		11.10 – 11.20	10	PRZERWA KAWOWA
5.		11.20 – 12.50	90	Podstawy zarządzania ryzykiem dla systemów zabezpieczeń w odniesieniu do międzynarodowych standardów
6.		12.50 – 13.45	55	PRZERWA OBIADOWA
7.		13.45 – 15.15	90	Architektura cyberbezpieczeństwa systemów zabezpieczeń technicznych i systemów ochrony przeciwpożarowej. Secure by design i secure by default.

L.p.	Dzień szkolenia	Godz. od - do	Czas trwania [min]	Temat wykładu/ćwiczeń
8.		15.15 – 15.25	10	PRZERWA KAWOWA
9.		15.25 – 16.10	45	Architektura cyberbezpieczeństwa systemów zabezpieczeń technicznych i systemów ochrony przeciwpożarowej. Secure by design i secure by default. Ciąg dalszy.

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 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.