Kod szkolenia: **HL945S**

Tytuł szkolenia: **Kluczowe Aspekty Bezpieczeństwa Informacji**

Information Security Essentials

Dni: 3

Authorized HP Training Reseller

Opis:

Ten trzy dniowy kurs przygotuje Cię do spojrzenia na Twój biznes przez pryzmat bezpieczeństwa i pozwoli przygotować spójną strategię bezpieczeństwa, która pozwoli utrzymać Twój biznes na odpowiednim poziomie w porównaniu do konkurencji. Kurs obejmuje najważniejsze koncepcje bezpieczeństwa i pokazując rzeczywiste przykłady jak wdrażać zabezpieczenia i minimalizować ryzyka w Twojej organizacji.

Cel szkolenia

Niezależnie od tego czy odpowiadasz za kierowanie, czy też za stronę techniczną bezpieczeństwa, ten kurs jest kluczowy abyś zrozumiał, czym jest bezpieczeństwo informacji uwzględniając zarzadzanie ryzykiem, techniczne i administracyjne zabezpieczenia, przepisy prawa, fizyczne i osobowe zabezpieczenia, standardy bezpieczeństwa (np. ISO 27001/2), utrzymanie ciągłości działania i wiele innych.

Szkolenie jest akredytowane przez wiele instytucji certyfikujących i przygotuje Cię do certyfikacji APMG-International ISO/IEC 27001 oraz do Information Security Foundation na bazie ISO/IEC 27002 (ISFS) (certyfikacja EXIN). Ponadto uczestnicząc dodatkowo w 2-dniowym kursie Information Security Essentials Plus (HL946S) przygotujesz się do egzaminu Certified Information Security Management Principles (CISMP) organizowanego przez BCS. Ten kurs dostarcza podstaw do bardziej zaawansowanych certyfikacji (takich jak CISSP, Security+ oraz CCSK) i odpowiada aktualnym programom zarządzania projektami i utrzymaniem.

Adresaci szkolenia

Szkolenie dedykowane jest osobom na stanowiskach kierowniczych w działach IT oraz członków Zespołów Zarządzania Bezpieczeństwem informacji, kierownikom, szefom bezpieczeństwa i systemów IT oraz każdemu kto przygotowuje się do uzyskania certyfikatu z zakresu ISO/IEC 27001, ISO/IEC 27002, CISMP, CISSP, Security+ or CCSK.

Wymagania

Podstawowa znajomość systemów operacyjnych i sieci IT.
Doświadczenie z zarządzania sieciami będzie pomocne, ale nie niezbędne.
Doświadczenie w zarządzaniu projektami oraz organizacją będzie pomocne, ale nie niezbędne.

Informacje dodatkowe

Szkolenie może być zrealizowane w języku polskim lub angielskim. Uczestnicy otrzymują akredytowane materiały szkoleniowe w języku angielskim.

Program szkolenia:

Moduł 1: Ustanowienie podstaw bezpieczeństwa.

- Przykłady jak ważne jest bezpieczeństwo informacji.
- Jak bezpieczeństwo może decydować o przewadze w businessie.
- Modele dojrzałości zapewnienie informacji.
- Identyfikacja właściwych źródeł wymogów zgodności prawnych, regulacyjnych, klienckich.

Moduł 2: Definicja kluczowych założeń bezpieczeństwa informacji.

- Bezpieczeństwo informacji oraz kluczowe elementy: poufność, integralność, dostępność.
- Spełnienie wymagań w bezpieczeństwie informacji.
- Różnice pomiędzy zagrożeniami, podatnościami a atakami.
- Zastosowanie definicji w środowisku.

- Identyfikacja form zagrożeń.
- Wykaz typowych podatności w firmach.
- Omówienie, co jest przyczyną incydentów bezpieczeństwa.

Moduł 3: Zarządzanie bezpieczeństwem informacji w organizacji.

- Wskazanie przewagi stosowania istniejących wytycznych.
- Pokazanie cyklu zarządzania bezpieczeństwem.
- Wskazanie kluczowych ról, odpowiedzialności i interakcji.
- Różnice pomiędzy polityką, standardem, procedurą a wytycznymi.
- Charakterystyka dobrej polityki.
- Jak ważne jest ogłoszenie polityki.

Moduł 4: Wprowadzenie do zagrożeń IT, podatności i ataków.

- Omówienie podatności w komunikacji klient/serwer
- Omówienie, dlaczego duże organizacje są zagrożone
- Identyfikacja fizycznych, technicznych i socjotechnicznych zagrożeń
- Identyfikacja i Omówienie najczęściej występujących ataków
- Omówienie najczęściej występujących przykładów ataków socjotechnicznych

Moduł 5: Ocena ryzyka.

- Role zarządzania ryzykiem w bezpieczeństwie informacji oraz ich powiązanie z cyklem zarządzania bezpieczeństwem.
- Szacowanie ryzyka szczątkowego dla Twojej organizacji w różnych kluczowych obszarach.
- Różnice pomiędzy analizą wpływu na działalność a ocena ryzyka.
- Różnice pomiędzy jakościowym a ilościowym analizowaniem ryzyka.
- Omówienie skanowania podatności.
- Przykładowe narzędzia do skanowanie portów komunikacyjnych oraz innych podatności.
- Wskazanie narzędzi kryteriów wyboru i porównania.
- Przygotowanie raportu ze skanowania.

Moduł 6: Kontrola dostępu.

- Omówienie wagi kontroli dostępu w implementacji bezpieczeństwa informacji
- Wskazanie jak autoryzacja i weryfikacja działają razem w celu zapewnienia kontroli dostępu
- Zarys, dlaczego techniczne i fizyczne zabezpieczenia są wspólnie bardzo ważne

Moduł 7: Wybór zabezpieczeń.

- Wskazanie typowych zabezpieczenia dla każdej z kategorii zagrożenia.
- Wskazanie przeciwdziałania ze względu na strategię.

- Omówienie ważności zarządzania aktualizacją i patchowaniem.
- Kategoryzacja zabezpieczeń fizycznych.
- Omówienie przeciwdziałania technicznego.
- Identyfikacja pozycji firewall w architekturze sieciowej i w strefie DMZ.
- Wskazanie działania, jakie firewall może podjąć w celu rozpoznania ruchu sieciowego.
- Omówienie działania IPS (Intrusion Prevention Systems).
- Omówienie jak IPS wykrywa atak.
- Porównanie typów IPS-ów.
- Omówienie jak VPN (Virtual Private Networking) wspiera cele bezpieczeństwa.
- Omówienie jak szyfrowanie wspiera bezpieczeństwo.
- Omówienie jak można stosować szyfrowanie.
- Różnice pomiędzy szyfrowaniem symetrycznym a asymetrycznym.
- Omówienie pozycjonowania skanerów antywirusowych.

>Moduł 8: Planowanie zabezpieczeń dla konsumeryzacji i rozwiązań Cloud (chmury obliczeniowej) w IT

- Omówienie wpływu konsumeryzacji IT.
- Omówienie zagrożenia i podatności dla rozwiązań mobilnych.
- Podsumowanie interwencji dla rozwiązań mobilnych.
- Identyfikacja zagrożeń ze strony mediów społecznościowych.
- Podsumuj zabezpieczenia dla mediów społecznościowych.
- Omówienie relacji pomiędzy konsumeryzacją a rozwiązaniami chmury obliczeniowej.
- Różnice pomiędzy rozwiązaniami chmury obliczeniowej i usługami.
- Identyfikacja ryzyka dla różnych przykładów wykorzystania chmury obliczeniowej.
- Przykłady zabezpieczeń dla chmury obliczeniowej.

Moduł 9: Planowanie utrzymania ciągłości działania oraz przywracanie po awarii.

- Omówienie ważności ciągłości działania.
- Przykłady, dlaczego jest to takie ważne.
- Omówienie ciągłości działania i terminów z tym związanych.
- Omówienie relacji z zarządzaniem ryzykiem.
- Wskazanie elementów utrzymania ciągłości działania.
- Porównanie i różnice pomiędzy BCP a DRP.
- Omówienie kluczowych elementów oraz prawne zapisy dostępności usług.
- Omówienie weryfikacji rozwiązań redundantnych.
- Rozważania na temat redundancji.

Moduł 10: Strategie wdrożenia dla właściwego poziomu bezpieczeństwa.

- Wskazanie kilku najczęściej pomijanych zagrożeń dla bezpieczeństwa IT.
- Wskazanie najlepszych praktyk w zakresie zatrudniania i szkolenia użytkowników/pracowników.