CYBERBEZPIECZEŃSTWO

- PODSTAWY

PRAKTYCZNY WARSZTAT

Termin: 8-10 listopada 2021 roku

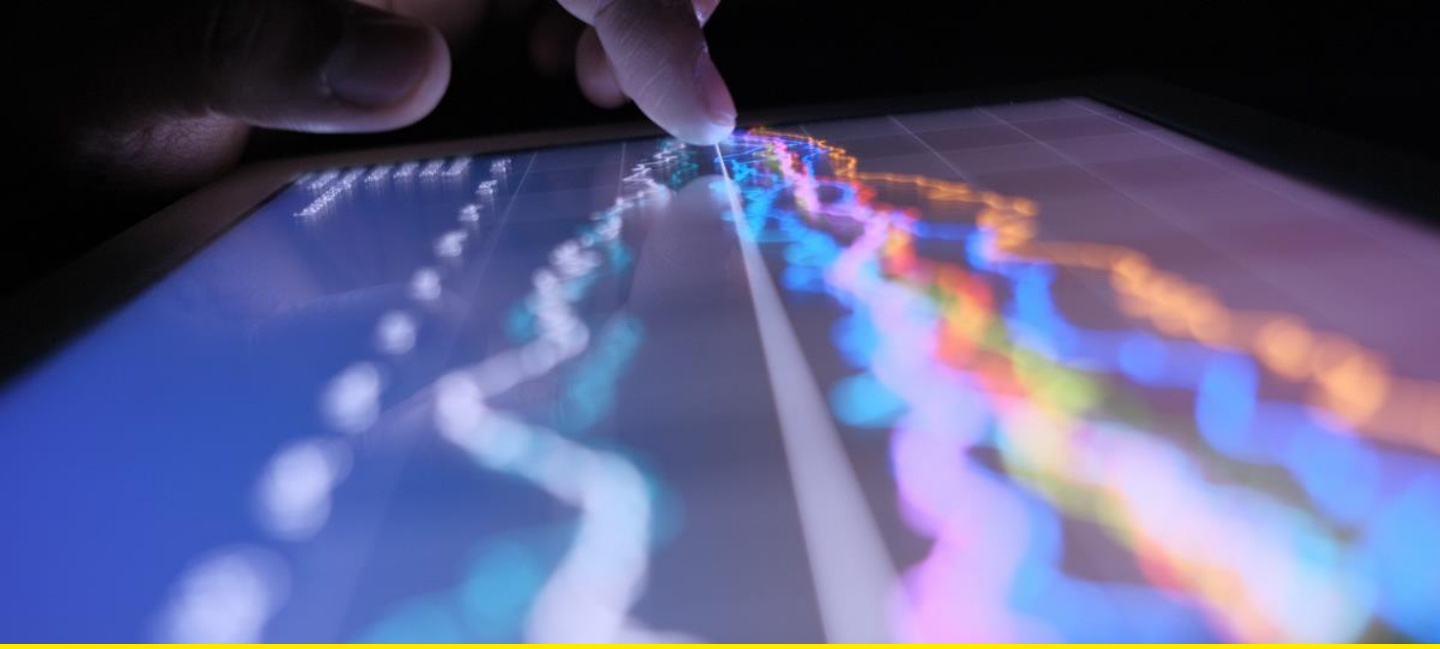
Online live lub stacjonarnie w Warszawie
(w zależności od sytuacji epidemicznej)

Kontakt:
Monika Kacprzykowska
+48 789 407 575
Monika.Kacprzykowska@pl.ey.com

academyofbusiness.pl

ACADEMY OF BUSINESS #1

EY
Building a better working world



Zajęcia kierujemy do:

- Szkolenie wprowadza w tematykę cyberbezpieczeństwa. Jest ono skierowane zarówno do pracowników działów IT, którzy nie mieli jeszcze do czynienia z tym tematem jak i do managerów pragnących zrozumieć podstawowe zasady bezpieczeństwa.
- Szkolenie dedykujemy również wszystkim, którzy chcą poszerzyć wiedzę z zakresu cyberbezpieczeństwa.

Korzyści i cele szkolenia:

- Zdobędziesz/poszerzysz wiedzę z zakresu szeroko rozumianego cyberbezpieczeństwa, dzięki czemu będziesz mógł podejmować lepsze decyzje biznesowe.
- Będziesz w stanie przeprowadzić świadomą ocenę sytuacji w swojej firmie.
- Zbudujesz umiejętność oceny zagrożeń i własnych zabezpieczeń.
- Zdobędziesz wiedzę z zakresu bezpieczeństwa systemów operacyjnych.
- Zrozumiesz na czym polega bezpieczeństwo w sieci oraz jak uchronić się przed złośliwym oprogramowaniem.
- Poznasz zasady dotyczące złożoności haseł.
- Poczujesz się pewniej w temacie cyberbezpieczeństwa.

Program

Zrozumienie podstawowych zasad bezpieczeństwa

Poufność; integralność; dostępność; wpływ zagrożenia i ryzyka; zasada najmniejszego przywileju; Inżynieria społeczna; analiza powierzchni ataku; modelowanie zagrożeń.

Zrozumienie bezpieczeństwa fizycznego

Bezpieczeństwo obiektu; bezpieczeństwo komputera; wymienne urządzenia i dyski; kontrola dostępu; bezpieczeństwo urządzeń mobilnych; keyloggery.

Zrozumienie bezpieczeństwa w Internecie

Ustawienia bezpieczeństwa przeglądarki; bezpieczne strony internetowe.

Zrozumienie bezpieczeństwa sieci bezprzewodowej

Zalety i wady konkretnych typów zabezpieczeń; Klucze; SSID; Filtry MAC.

Zrozumienie bezpieczeństwa systemu operacyjnego

Zrozumienie uwierzytelniania użytkowników; uwierzytelnianie wieloskładnikowe; fizyczne i wirtualne smart cardy; Usługa zdalnego uwierzytelniania użytkowników (RADIUS); biometria; użycie opcji „Uruchom jako", do wykonywania zadań administracyjnych

Zrozumienie uprawnień

Uprawnienia systemu plików; uprawnienia udostępniania; Registry; Active; Directory; włączanie i wyłączanie dziedziczenia; zachowanie podczas przenoszenia lub kopiowania plików na tym samym dysku lub na inny dysk; wiele grup z różnymi uprawnieniami; uprawnienia podstawowe i uprawnienia zaawansowane; przejecie własności; delegacja; dziedziczenie

Zrozumienie zasad dotyczących haseł

Złożoność hasła; blokada konta; długość hasła; historia haseł; czas między zmianami hasła; egzekwowanie za pomocą Zasad Grupy; powszechne metody ataku; procedury resetowania hasła; ochrona haseł do kont użytkowników domeny.

Zrozumienie zasad audytu

Rodzaje audytów; co może podlegać audytowi; włączanie audytu; co audytować w określonych celach; gdzie zapisywać informacje audytowe; jak zabezpieczać informacje audytowe.

Zrozumienie szyfrowania

System szyfrowania plików (EFS); wpływ folderów zaszyfrowanych przez EFS na przenoszenie / kopiowanie plików; BitLocker (To Go); TPM; szyfrowanie oparte na oprogramowaniu; szyfrowanie i podpisywanie poczty mail oraz inne zastosowania; wirtualna sieć prywatna (VPN); klucz publiczny / klucz prywatny; algorytmy szyfrowania; właściwości certyfikatu; usługi certyfikujące;
Infrastruktura PKI / usługi certyfikacyjnych; tokeny sprzętowe, ograniczenie urządzeń, aby uruchamiały tylko zaufane aplikacje.

Zrozumienie złośliwego oprogramowania

Przepełnienie bufora; wirusy, wirusy polimorficzne; robaki; Konie trojańskie; programy szpiegujące; oprogramowanie ransomware; oprogramowanie reklamowe; rootkity; tylne drzwi; ataki zero day.

Program cd.

Zrozumienie dedykowanych zapór ogniowych

Rodzaje zapór sprzętowych i ich charakterystyka; kiedy używać zapory sprzętowej zamiast zapory opartej na oprogramowaniu; inspekcja stanowa i bezstanowa; podstawy bezpieczeństwa

Zrozumienie izolacji sieci

Trasowanie; honeypot; sieci obwodowe; translacja adresów sieciowych (NAT); VPN; IPsec; izolacja serwerów i domen.

Zrozumienie zabezpieczenia protokołów

Spoofing protokołów; IPsec; tunelowanie; DNSsec; podsłuchiwanie sieci; ataki typu DoS; powszechne metody ataku.

Zrozumienie ochrony stacji klienckich

Antywirus; ochrona przed niechcianymi instalacjami oprogramowania; kontrola.

konta użytkownika (UAC); aktualizacja systemu operacyjnego klienta i oprogramowania klienta; szyfrowanie folderów offline, zasady ograniczeń oprogramowania; zasada najmniejszego przywileju

Zrozumienie ochrony poczty elektronicznej

Antyspam, oprogramowanie antywirusowe, spoofing, phishing i pharming; ochrona.

klienta a ochrona serwera; Rekordy Sender Policy Framework (SPF); Rekordy PTR.

Zrozumienie ochrony serwera

Rozdzielenie usług; hartowanie (hardening); aktualizacje serwera; bezpieczne.

aktualizacje dynamicznego systemu nazw domen (DNS); dezaktywacja niezabezpieczonych protokołów uwierzytelniania; Kontrolery domeny tylko do odczytu (RODC).

INFORMACJE
organizacyjne

Miejsce i godziny

Warszawa, Centrum Szkoleniowe
EY Academy of Business, budynek Focus,
al. Armii Ludowej 26. Szkolenie odbywa się
w godz. 9:00-16:30.

Lub ONLINE LIVE (przekaz w czasie rzeczywistym)

- Pełna oferta naszych szkoleń znajduje się na stronie: academyofbusiness.pl
- Promocje, nowości, wydarzenia: www.facebook.com/EYszkolenia
- Obserwuj EY Academy of Business na LinkedIn i bądź na bieżąco

Wypełnij zgłoszenie on-line!

Cena

Koszt kursu stacjonarnego wraz
z materiałami wynosi **2950 zł + 23% VAT**.

Opłaty należy wnieść przed rozpoczęciem kursu na podstawie faktury pro-forma.
Po dokonaniu płatności każdy uczestnik otrzyma fakturę VAT.

Kontakt

Monika Kacprzykowska
Specjalista ds. sprzedaży
tel. +48 789 407 575
Monika.Kacprzykowska@pl.ey.com

Dla firm

Oferujemy również realizację szkolenia
w formule in-house (grupa zamknięta,
wyłącznie dla pracowników Państwa firmy).