MICHAŁ TOPOLSKI – OFERTA SZKOLEŃ Z CYBERBEZPIECZEŃSTWA

O MNIE

Nazywam się **Michał Topolski** i jestem studentem **cyberbezpieczeństwa** na Politechnice Warszawskiej. Fascynacja tą dziedziną towarzyszy mi od dawna. Posiadam bogate doświadczenie w prowadzeniu szkoleń i prelekcji zdobyte w organizacjach trzeciego sektora. Łączę je z **wiedzą i praktycznym doświadczeniem technicznym** – tworzyłem strony internetowe i aplikacje oraz zarządzałem systemami IT w małych i średnich podmiotach, w tym w organizacji liczącej **ponad 20 000** członków. W pracy z ludźmi stawiam na **praktyczne umiejętności,** dlatego moje szkolenia są interaktywne i zawierają wiele elementów warsztatowych.

Poza wymienionym wyżej doświadczeniem angażuję się społecznie jako instruktor Związku Harcerstwa Rzeczypospolitej, prowadzę szkolenia z debat oksfordzkich, aktywnie debatuję i sędziuję debaty, okazjonalnie tworzę grafiki – logotypy i identyfikacje wizualne.

SZKOLENIA

Moje szkolenia rozpoczynają się wprowadzeniem do świata cyberbezpieczeństwa, a następnie obejmują trzy główne obszary tematyczne: **sprzęt, oprogramowanie oraz ludzi**. Bez względu na specyfikę instytucji i branży, te elementy zawsze tworzą system obiegu informacji i wpływają na poziom bezpieczeństwa. Różnica leży w tym jakie konkretnie sprzęty i oprogramowanie obsługują ludzie (i ilu tych ludzi jest) w naszej organizacji, oraz jakimi danymi operujemy. To sprawia, że każde szkolenie opiera się na uniwersalnym fundamencie i omawia podobne zagadnienia.

Każdy program szkoleniowy trwa standardowo 6 godzin i jego zakres może być dostosowany do potrzeb konkretnej grupy odbiorców.

Szkolenie dla placówek oświatowych

Sugerowany czas trwania: 6 godzin

Wstęp: Czym jest cyberbezpieczeństwo? Po co dbać o cyberbezpieczeństwo? Czy komuś chce się atakować oświatę? Jakie dane przetwarzamy? Dlaczego należy bać się wiewiórek?

Sprzęt: Jak dbać o bezpieczeństwo komputerów służbowych? Czy sale informatyczne i uczniowie są źródłem zagrożenia? Jak bezpiecznie korzystać z publicznego wi-fi? Jak groźny może być zwykły pendrive? Czy drukarka może być naszym czułym punktem? Kto podgląda nas przez kamerkę? Czym są klucze sprzętowe?

Oprogramowanie: Discord, Messenger, Telegram, Signal, Whatsapp i inne komunikatory – jak bezpieczenie z nich korzystać? Czym są menadżery haseł? Czym jest deep web i dark web? Czym różni się wirus od trojana? Jakie hasło to silne hasło?

Ludzie: Jak nie dać się oszukać? Czym jest phishing? Skąd wiedzieć, czy ktoś jest tym za kogo się podaje? Jak kształtować kulturę bezpiecznej organizacji? Jak rozpoznać dezinformację? Co to socjotechnika?

Szkolenie z elementami warsztatowymi, przy odpowiedniej ilości uczestników proponuję ćwiczenia praktyczne w mniejszych grupach.

Szkolenie dodatkowo można uzupełnić i rozszerzyć m. in. o zagadnienia dotyczące higieny cyfrowej, zagrożeń dla młodzieży w internecie (handel nielegalnymi substancjami, drastyczne treści itd.), profilaktyki zagrożeń i wyzwań związanych z SI.

Szkolenie dla placówek medycznych

Sugerowany czas trwania: 6 godzin

Wstęp: Czym jest cyberbezpieczeństwo? Dlaczego cyberbezpieczeństwo jest kluczowe w ochronie zdrowia? Czy placówki medyczne są atrakcyjnym celem dla cyberprzestępców? Jakie dane przetwarzamy i dlaczego są one cenne? Jakie są potencjalne skutki wycieku danych pacjentów? Jak uczyć się na cudzych błędach? Dlaczego należy bać się wiewiórek?

Sprzęt: Jak dbać o bezpieczeństwo komputerów służbowych? Jak bezpiecznie korzystać z sieci Wi-Fi w placówkach medycznych? Czy urządzenia medyczne mogą być celem cyberataków? Jak bezpiecznie korzystać z publicznego wi-fi? Czym są klucze sprzętowe?

Oprogramowanie: Jak bezpiecznie korzystać z systemów zarządzania informacjami medycznymi (EMR/EHR)? Jak zabezpieczać komunikację w pracy? Czym są menadżery haseł? Czym różni się ransomware od innych typów złośliwego oprogramowania i dlaczego właśnie placówki medyczne są najbardziej narażone na tego typu ataki? Jakie hasło to silne hasło?

Ludzie: Jak nie dać się oszukać? Czym jest phishing? Skąd wiedzieć, czy ktoś jest tym za kogo się podaje? Jak kształtować kulturę bezpiecznej organizacji? Jak rozpoznać dezinformację? Co to socjotechnika? Jak kontrolować dostęp do pomieszczeń?

Szkolenie z elementami warsztatowymi, przy odpowiedniej ilości uczestników proponuję ćwiczenia praktyczne w mniejszych grupach.

Szkolenie dodatkowo można uzupełnić i rozszerzyć m. in. o analizę głośnych ataków na placówki ochrony zdrowia i bazy danych ubezpieczycieli (studium przypadków) lub zagadnienia z dziedziny cyberbiobezpieczeństwa.

Szkolenie dla samorządów i instytucji publicznych

Sugerowany czas trwania: 6 godzin

Wstęp: Czym jest cyberbezpieczeństwo? Dlaczego instytucje publiczne muszą dbać o cyberbezpieczeństwo? Jakie podmioty najczęściej są celem cyberataków? Jakie dane

przetwarzamy i dlaczego są one ważne? Jakie są potencjalne konsekwencje wycieku danych? Jak radzić sobie w czasach kryzysu? Dlaczego należy bać się wiewiórek?

Sprzęt: Jak zabezpieczyć komputery i serwery w instytucjach publicznych? Jak bezpiecznie korzystać z publicznego Wi-Fi? Jakie zagrożenia mogą wynikać z używania nośników danych (np. pendrive'ów)? Czy drukarki, skanery i urządzenia wielofunkcyjne mogą być celem cyberataków? Jak chronić prywatność podczas wideokonferencji? Czym są klucze sprzętowe?

Oprogramowanie: Jak zabezpieczać komunikację wewnątrz zespołu? Jak prowadzić bezpieczną korespondencję zewnętrzną? Czym są menadżery haseł i jak mogą nam pomóc? Jakie istnieją rodzaje złośliwego oprogramowania i które najbardziej nam zaszkodzi? Jakie hasło to silne hasło?

Ludzie: Jak nie dać się oszukać? Czym jest phishing? Skąd wiedzieć, czy ktoś jest tym za kogo się podaje? Jak kształtować kulturę bezpiecznej organizacji? Jak rozpoznać dezinformację? Co to socjotechnika? Jak chronić naszych interesantów?

Szkolenie z elementami warsztatowymi, przy odpowiedniej ilości uczestników proponuję ćwiczenia praktyczne w mniejszych grupach.

Szkolenie dodatkowo można uzupełnić i rozszerzyć m. in. o demonstrację hipotetycznego ataku na instytucję, doktrynę cyber-przetrwania, omówienie scenariuszy konkretnych zagrożeń, zagadnienie zwalczania dezinformacji.

Szkolenie dla firm

Sugerowany czas trwania: 6 godzin

Wstęp: Czym jest cyberbezpieczeństwo? Dlaczego cyberbezpieczeństwo jest kluczowe dla firm? Jakie podmioty najczęściej są celem cyberataków? Jakie dane przetwarzamy i dlaczego są one cenne? Jakie są potencjalne skutki wycieku danych firmowych? Jak uczyć się na cudzych błędach? Dlaczego należy bać się wiewiórek?

Sprzęt: Jak dbać o bezpieczeństwo komputerów służbowych? Jak bezpiecznie korzystać z sieci Wi-Fi w firmie? Jak zabezpieczać służbowe i prywatne urządzenia mobilne? Jak bezpiecznie korzystać z publicznego Wi-Fi? Czym są klucze sprzętowe i jak je stosować? Jakie zagrożenia mogą wynikać z używania nośników danych (np. pendrive'ów)? Jak chronić prywatność podczas wideokonferencji?

Oprogramowanie: Jak bezpiecznie korzystać z systemów informatycznych? Jak zabezpieczać komunikację wewnątrz firmy? Czym są menadżery haseł i jak mogą nam pomóc? Jakie istnieją rodzaje złośliwego oprogramowania i które najbardziej nam zaszkodzi? Jakie hasło to silne hasło? Jakie aplikacje i programy są najczęściej celem ataków?

Ludzie: Jak nie dać się oszukać? Czym jest phishing i jak go rozpoznać? Skąd wiedzieć, czy ktoś jest tym, za kogo się podaje? Jak kształtować kulturę bezpiecznej organizacji? Jak rozpoznać dezinformację? Co to socjotechnika i jak się przed nią bronić? Czy trzeba kontrolować dostęp do pomieszczeń biurowych?

Szkolenie z elementami warsztatowymi, przy odpowiedniej ilości uczestników proponuję ćwiczenia praktyczne w mniejszych grupach.

Szkolenie dodatkowo można uzupełnić i rozszerzyć o analizę głośnych ataków na firmy i korporacje (studium przypadków), higienę cyfrową i prywatność w sieci, omówienie scenariuszy konkretnych zagrożeń, zwalczanie dezinformacji i fake news, cyberbezpieczeństwo w dobie pracy zdalnej, biały wywiad i ochronę danych firmowych w sieci.

Szkolenie tematyczne na zamówienie

Sugerowany czas trwania: od 3 do 8 godzin

Oferuję także szkolenia skupiające się na pojedynczym zagadnieniu lub o rozszerzonym zakresie według potrzeb klienta. Przykładowe tematy szkoleń: „Największe mity cyber- (i nie tylko) bezpieczeństwa", „Ile można odczytać z naszych publicznych danych – biały wywiad i prywatność w sieci".

ROZLICZENIA I FORMALNOŚCI

Zależnie od zapotrzebowania szkolenie prowadzę na podstawie umowy zlecenie lub wystawiam fakturę VAT. Koszty szkoleń ustalam indywidualnie, gdyż zależą od wielu czynników – zapraszam serdecznie do kontaktu.

KONTAKT

Adres e-mail: michal@topolski.xyz

Numer telefonu: (+48) 508 287 490