Szkolenie Security awareness - Analiza zagrożeń cyfrowych

Opis szkolenia: Wprowadzenie do zagadnień, związanych z cyberbezpieczeństwem, także tych zaawansowanych i włączenie praktycznych warsztatów, które utrwalą nabytą wiedzę. Zapoznanie ze złośliwym oprogramowaniem, na które można napotkać w codziennym życiu.

Kod szkolenia: SEC-ZAGR-01

Kategoria: Security awareness / Cyberbezpieczeństwo / Edukacja pracowników

Trenerka: Beata Zalewa

Czas trwania: 4 godziny (np. 9:00 – 13:00)

Poziom zaawansowania: Podstawowy

Język wykładowy: język polski

Forma szkolenia: zdalne. Po wcześniejszym uzgodnieniu możliwe szkolenie w siedzibie klienta.

Materiały: w języku polskim. Na życzenie klienta materiały w języku angielskim.

Wymagania wstępne: Brak - szkolenie dla każdego pracownika.

Grupa decelowa: Pracownicy różnych branż. Szkolenie może być dopasowane pod konkretną branżę.

Cel szkolenia: Zrozumienie zaawansowanych zagrożeń cyfrowych.

Efekty szkolenia:

- Uczestnik zna najpopularniejsze techniki manipulacji oraz współczesne wektory ataków socjotechnicznych, takie jak phishing, smishing, vishing czy identity theft (kradzież tożsamości).
- Uczestnik potrafi skutecznie identyfikować podejrzane wiadomości e-mail, zmanipulowane linki oraz próby wyłudzenia danych w codziennej komunikacji biznesowej, a także właściwie zgłaszać wykryte incydenty.
- Uczestnik potrafi wdrożyć w praktyce zasady higieny cyfrowej, obejmujące m.in. silne uwierzytelnianie (MFA), bezpieczne korzystanie z sieci publicznych oraz fizyczną i systemową ochronę stanowiska pracy.
- Uczestnik rozumie psychologiczne mechanizmy (takie jak presja czasu, autorytet czy strach), którymi posługują się cyberprzestępcy, aby uśpić czujność ofiary.
- Uczestnik rozumie, że czynnik ludzki jest najczęstszym celem ataków, a jego indywidualna odpowiedzialność i codzienne nawyki mają bezpośredni wpływ na bezpieczeństwo i stabilność całej organizacji.

Co otrzymasz?

- Materiały szkoleniowe.
- Szkolenie kończy się certyfikatem uczestnictwa.

Agenda szkolenia

Godzina	Czas trwania	Moduł	Forma
9:00 - 9:20	20 minut	Wstęp i przedstawienie podstawowych pojęć z zakresu phishingu, haseł i malware	Studium przypadku, dyskusja
9:20 - 10:05	45 minut	Inżynieria społeczna – zaawansowane techniki i symulacje	Studium przypadku, dyskusja
10:05 - 10:50	45 minut	Warsztat symulacyjny: Testy phishingowe	Studium przypadku, dyskusja
10:50 - 11:00	10 minut	Przerwa kawowa	-
11:00 - 11:45	45 minut	Złośliwe oprogramowanie – głębokie zanurzenie	Studium przypadku, dyskusja
11:45 - 12:15	30 minut	Bezpieczeństwo poza biurem i w pracy zdalnej	Studium przypadku, dyskusja
12:15 - 12:45	30 minut	Warsztat: Analiza incydentu	Studium przypadku, dyskusja
12:45 - 13:00	15 minut	Sesja pytań i odpowiedzi	Q&A, ankieta końcowa

Szczegółowy program szkolenia

Moduł 1: Wstęp

Wprowadzenie do tematu i przedstawienie agendy.

- Przedstawienie prowadzącego i uczestników.
- Omówienie celów i struktury szkolenia.
- Zasady współpracy i interaktywności.
- Przedstawienie podstawowych pojęć z zakresu phishingu, haseł i malware.

Moduł 2: Inżynieria społeczna – zaawansowane techniki i symulacje

- Whaling: Ataki skierowane na kluczowych decydentów w firmie, np. próby wyłudzenia przelewów na podstawie sfałszowanych wiadomości od prezesa.
- Pretexting: Tworzenie fałszywych scenariuszy w celu wyłudzenia informacji, np. podawanie się za pracownika pomocy technicznej.
- Baiting: Wykorzystanie ludzkiej ciekawości do zainfekowania urządzenia, np. przez pozostawienie nośnika USB z intrygującą nazwą pliku.

Moduł 3: Warsztat symulacyjny: Testy phishingowe

- Praktyczna symulacja ataku phishingowego, dostosowana do poziomu uczestników.
- Od prostych e-maili z prośbą o reset hasła do bardziej zaawansowanych, spersonalizowanych wiadomości.
- Analiza błędów i omówienie, w jaki sposób takie testy pomagają w budowaniu świadomości i utrwalaniu poprawnych nawyków.

Moduł 4: Złośliwe oprogramowanie – głębokie zanurzenie

- Szczegółowe omówienie złośliwego oprogramowania: ransomware, trojany, rootkity, botnety, robaki oraz nowsze zagrożenia, takie jak fileless malware (działające w pamięci komputera) i wiper malware (trwale usuwające dane).
- Wytłumaczenie, jak działają i jakie są ich cele, od kradzieży danych po sabotaż.

Moduł 5: Bezpieczeństwo poza biurem i w pracy zdalnej

- Omówienie zagrożeń związanych z publicznymi sieciami Wi-Fi.
- Wskazanie na ryzyka związane z bezpieczeństwem urządzeń mobilnych, takich jak smartfony i laptopy. Wytłumaczenie, jak działają ataki na telefony (np. SIMswap fraud) i mobilne malware.

Moduł 6: Warsztat: Analiza incydentu

- Uczestnicy pracują w grupach nad analizą przykładowego scenariusza incydentu (np. wyłudzenie dostępu do konta firmowego).
- Ćwiczenie to ma na celu praktyczne przećwiczenie procedur reagowania na zagrożenie i podjęcie szybkich, właściwych decyzji.

Moduł 7: Podsumowanie, Q&A i kolejne kroki

- Podsumowanie i wnioski.
- Sesja pytań i odpowiedzi.
- Ankieta końcowa i informacje o certyfikacie.

Zarejestruj się na szkolenie: szkolenia@zalnet.pl

https://zalnet.pl/edu/analiza-zagrozen-cyfrowych/

ZALNET
Beata Zalewa

+48 600 926 031
info@zalnet.pl
www.zalnet.pl

Wola Radzięcka 62
23-440 Frampol
NIP 717 111 99 64