EDUHEZO

Jak rozpoznać cyberzagrożenia?

EXCLUSIVE NETWORKS

all of security

Oszustwa, kradzieże czy porwania dla okupu – to zjawiska, które towarzyszą ludzkości od zarania dziejów.

Na przestrzeni czasów nieustannie zmieniają się i są doskonalone. Każde z tych działań występowało i występuje w wersjach bardzo prostych, ale także i w bardzo wyrafinowanych.

Oszuści, złodzieje i porywacze działają nieustannie, a liczba „operacji" przez nich wykonywanych, z roku na rok rośnie. W coraz mniejszym stopniu takie działania wykonywane są w sferze rzeczywistej. Przestępcy przenieśli się do internetu i strefy wirtualnej, gdzie działają odważniej i bardziej niebezpiecznie niż kiedykolwiek.

Kieszonkowcy, którzy kiedyś pojawiali się w ruchliwych miejscach publicznych, teraz starają się okradać nasze konta bankowe. Przestępcy zajmujący się dawniej porwaniami, teraz przejmują kontrolę nad naszymi danymi i naszą tożsamością.

Oszuści podszywają się pod bliskie nam osoby czy zaufane instytucje, by zmylić naszą czujność i bardzo szybko oczyścić nasze konta z wszelkich oszczędności lub nas zadłużyć. Niezabezpieczone konto można okraść o wiele szybciej niż mieszkanie.

Działalność ta przeniesiona do strefy wirtualnej, nie ma już fizycznych granic.

W cyberświecie odległość geograficzna nie ma znaczenia. Haker z drugiego końca globu jest tak samo blisko nas w sferze wirtualnej, jak nasze dzieci czy współpracownicy w pokoju obok. Równie ważna, jak posiadanie zabezpieczeń fizycznych (w postaci firewalla, UTM-a, systemów ochrony poczty oraz systemu backupowego) jest świadomość zagrożeń, na jakie narażeni są użytkownicy (pracownicy). To na nich i do nich skierowanych jest najwięcej ataków.

Zawsze pośrodku między pierwszą linią obrony (firewalle) a ostatnią deską ratunku (backup) istnieje element najbardziej wrażliwy i podatny – CZŁOWIEK = UŻYTKOWNIK. To właśnie umysł ludzki jest najmniej odporny na „zakłócenia", najtrudniej go uaktualnić i sprawić by wyuczone polityki były realizowane zawsze z taką samą pewnością.

Czy wiesz że:

84%

wszystkich ataków cybersecurity w 2021 było dystrybuowanych przez pocztę [1]

88%

personelu medycznego otwiera maile z phishingiem (dane za 2021 rok) [2]

95%

wszystkich incydentów zagrażających bezpieczeństwu IT ma związek z tzw. czynnikiem ludzkim [3]

o 300%

wzrosła liczba użytkowników atakowanych przy użyciu phisingu w państwach NATO przez rosyjskich hakerów w 2022 roku [4]

o 435%

wzrosło zastosowanie programów szyfrujących dane (ransomware) do wymuszeń okupu od 2020 roku [5]

1 Raport Sophos o cyberbezpieczeństwie 2022
2 Raport Sophos o cyberbezpieczeństwie 2022
3 Raport IBM o cyberbezpieczeństwie 2022
4 Raport Google: Fog of War 2023-02-16
5 Badanie ESI ThoughLab 2022

Większość ataków skierowana jest na

ludzi – nie na sprzęt

Oprócz zapory ogniowej i backupu, powinniśmy przede wszystkim dbać o jak największą świadomość użytkowników, których chronimy. Tylko w ten sposób zabezpieczymy się przed próbami wyłudzenia, zainfekowania i kradzieży.

Jednym z najważniejszych działań defensywnych jest obecnie edukacja nietechnicznych pracowników, którzy obsługują klientów, używają komputerów, urządzeń mobilnych i telefonów.

Szkolenia te koncertują się na podnoszeniu świadomości zagrożeń i wyrobieniu nawyku bycia podejrzliwym wobec wszelkich interakcji w internecie.

Skuteczna edukacja powinna być prowadzona w sposób dostosowany do możliwości i dostępnego czasu użytkowników.

Nauka przyzwyczajeń lub ich zmiana powinna być realizowana przede wszystkim:

- **w małych dawkach** – kilku/kilkunastominutowe moduły zapewniające wysokie przyswojenie przekazywanej wiedzy
- **w sposób interaktywny** – tak by zweryfikować poprawne zrozumienie podawanych informacji
- **w dogodnym momencie** – to użytkownik powinien wybrać czas, w którym może je wykonać
- **w przejrzysty i zrozumiały sposób** – bez trudnych pojęć i skrótów

Tak przeprowadzony proces daje najlepsze efekty.

Szkolenia z zakresu świadomości zagrożeń cyberbezpieczeństwa, są równie ważne jak dbanie o aktualizację wiedzy pracowników z zakresu ich obowiązków.

eduHEZO Jak rozpoznać cyberzagrożenia

to usługa bazująca na platformie ProofPoint Security Awareness, zapewniająca kompleksowy proces szkoleniowy obejmujący:

- zarządzanie i obsługę całego cyklu edukacyjnego
- koordynację i nadzór nad procesem
- bieżące raportowanie stanu realizacji
- ukierunkowane na uczestników kampanie phishingowe
- certyfikaty

a dodatkowo:

- uzupełniające moduły szkoleniowe dla użytkowników, którzy „złapią się na wędkę”
- powtórki szkoleń dla uczestników, którzy nie mogli ich wykonać lub chcą je zrealizować ponownie.

to ponad 50 interaktywnych szkoleń dostępnych w języku polskim, podzielonych na kategorie:

- bezpieczeństwo poczty email
- phishing
- bezpieczeństwo w internecie
- socjotechnika
- bezpieczeństwo pracy
- dane osobowe
- regulacje prawne

Cykl szkoleń eduHEZO – Jak rozpoznawać cyberzagrożenia? dostępny jest w dwóch modelach:

eduHEZO 3M

trzymiesięczny cykl zapewniający minimum 30 modułów szkoleniowych z zakresu podstawowego i rozszerzonego. Program zakłada przydzielanie tygodniowo od 2 do 4 szkoleń, które łącznie zajmują użytkownikom około pół godziny tygodniowo. Każdy moduł kończy się krótkim testem, którego ukończenie zapewnia zaliczenie szkolenia.

eduHEZO 6M

półroczny kompleksowy cykl edukacyjny, zapewniający pełny zakres szkoleń, które mogą być dopasowane do grup uczestników i przypisane dowolnie, w zależności od ich wiedzy, stanowiska i umiejętności. Szkolenia są rozłożone w dłuższym okresie, w zależności od dostępności i planów użytkowników.

Skontaktuj się z nami

edu@myHEZO.pl | myHEZO.pl/edu

Całość obsługi i nadzór jest realizowana przez zespół myHEZO przy minimalnym udziale zlecającego – dzięki temu, użytkownik nie musi sam uczyć się obsługi platformy i może zaufać najlepszym praktykom i doświadczeniu zespołu myHEZO.

Koordynator usługi po stronie zamawiającego otrzymuje na bieżąco najświeższe dane o postępach w szkoleniach, może modyfikować kolejność i harmonogram oraz wpływać na kształt realizowanego w tle phishingu.

Oprócz samych szkoleń, które są podstawowym elementem kursu, drugim ważnym aspektem są akcje phishingowe. Są to kampanie mailowe wysyłane do uczestników szkoleń, w postaci odpowiednio spreparowanych wiadomości, w których możemy podszyć się pod osoby z wewnątrz organizacji, dostawców lub instytucje publiczne. Maile te mają na celu nakłonić użytkownika do kliknięcia linku, wypełnienia danych na fikcyjnej stronie lub pobrania załącznika i uruchomienia go. Treści są przygotowywane na bazie wzorców posiadanych przez zamawiającego lub zgromadzonych przykładów w bazie eduHEZO.

EDU HEZO

Jak rozpoznać cyberzagrożenia?

EXCLUSIVE NETWORKS

all of security