Karta Pracy Studenta – Zajęcia 6

Temat: Złośliwe Oprogramowanie i Współczesne Scamy

Cel: Poznam najpopularniejsze rodzaje złośliwego oprogramowania (malware) i oszustw (scamów) oraz nauczę się, jak weryfikować bezpieczeństwo plików.

Wprowadzenie: Świat cyfrowy pełen jest zagrożeń – od prostych wirusów po zaawansowane oprogramowanie szyfrujące dane dla okupu (ransomware). Często kluczowym elementem ataku jest człowiek, którego oszuści manipulują, by sam zainstalował złośliwy program. Dziś nauczymy się, jak się przed tym bronić.

Ćwiczenie 1: Analiza studium przypadku (30 min)

Przeczytajcie w grupie opis zagrożenia, który otrzymaliście od prowadzącego. Odpowiedzcie na poniższe pytania.

Nazwa zagrożenia:

...

Jaki był cel ataku/oszustwa? (np. kradzież pieniędzy, zaszyfrowanie danych, kradzież tożsamości)

...

Jaka była metoda działania sprawców? (np. luka w oprogramowaniu, inżynieria społeczna, fałszywy link)

...

Jakie były skutki dla ofiar?

...

Jak można było się uchronić przed tym atakiem? (np. aktualizacje, niepodawanie kodów, weryfikacja)

...

Ćwiczenie 2: Prześwietlamy pliki z VirusTotal (25 min)

Pobierz plik testowy EICAR ze strony eicar.org, zgodnie z instrukcją prowadzącego. Plik ten jest nieszkodliwy, ale został stworzony, aby być wykrywanym przez antywirusy.

Wejdź na stronę virustotal.com.

Wybierz zakładkę "File", kliknij "Choose file" i wskaż pobrany plik.

Poczekaj na zakończenie analizy. Zapisz wynik.

Jaki był wynik skanowania (np. 65/70)?

...

Co ten wynik oznacza?

...

Pytanie: Wyobraź sobie, że dostałeś mailem plik "Faktura.exe". Twój antywirus na komputerze nic nie wykrył. Czy po dzisiejszych zajęciach uruchomiłbyś ten plik, czy wolałbyś go najpierw sprawdzić w VirusTotal? Uzasadnij.

...

Zasada bezpieczeństwa

Nie ufaj załącznikom, których się nie spodziewałeś. Zawsze miej zaktualizowany system operacyjny i program antywirusowy. Używaj VirusTotal do weryfikacji podejrzanych plików.