Karta Pracy Studenta – Zajęcia 7

Temat: Warsztat Analityczny – Rozwiązywanie Cyfrowej Zagadki

Cel: Wykorzystam w praktyce wiedzę z poprzednich zajęć, aby przeanalizować potencjalny incydent bezpieczeństwa i sformułować rekomendacje.

Wprowadzenie: Dziś jesteście zespołem analityków. Wasz klient otrzymał podejrzaną wiadomość i prosi Was o pomoc. Waszym zadaniem jest zbadanie sprawy i przygotowanie poniższego raportu.

Raport z Analizy Incydentu Bezpieczeństwa

Data: 24.09.2025

Zespół analityczny: ...

Dla: Klienta (Mały Przedsiębiorca)

Temat: Analiza podejrzanej wiadomości e-mail z dnia 24.09.2025

1. Streszczenie

Na podstawie analizy przedstawionych materiałów stwierdzamy, że wiadomość e-mail jest próbą oszustwa (phishingu), mającą na celu prawdopodobnie zainfekowanie komputera złośliwym oprogramowaniem i/lub wyłudzenie danych.

2. Analiza Materiału Dowodowego

A. Analiza wiadomości e-mail:

Zidentyfikowaliśmy następujące sygnały ostrzegawcze ("czerwone flagi"):

...

...

...

B. Analiza linku zawartego w wiadomości:

Po sprawdzeniu linku ustaliliśmy, że prawdziwy adres docelowy to: ...

Analiza domeny w bazie WHOIS wykazała, że: ...

C. Analiza załącznika (Wezwanie.docx):

Analiza metadanych pliku wykazała następujące informacje:

Autor: ...

Data utworzenia: ...

Skan pliku w serwisie VirusTotal wykazał, że: ...

3. Ocena Zagrożenia

Połączone wyniki analizy wskazują na wysokie prawdopodobieństwo, że:

Link prowadzi do fałszywej strony internetowej.

Załącznik zawiera złośliwe oprogramowanie (np. trojana, ransomware).

4. Rekomendacje (Co należy zrobić?)

Rekomendujemy podjęcie natychmiastowych działań:

Działania natychmiastowe:

NIE KLIKAĆ w link i NIE OTWIERAĆ załącznika.

Trwale usunąć wiadomość e-mail ze skrzynki.

...

Działania prewencyjne na przyszłość:

Przeszkolić pracowników w zakresie rozpoznawania phishingu.

Zawsze weryfikować tożsamość nadawcy w przypadku nieoczekiwanych wiadomości (np. telefonicznie).

...