Phishing jako zagrożenie cyberbezpieczeństwa – analiza i raportowanie incydentu

Internet oferuje wiele możliwości nauki w zakresie cyberbezpieczeństwa. W niniejszej pracy skupiam się na **phishingu**, czyli jednym z najczęściej spotykanych ataków hakerskich opartych na **social engineeringu**.

Phishing polega na tym, że ofiara otrzymuje wiadomość e-mail, która imituje legalną komunikację (np. bank, sklep internetowy, firma kurierska). Celem ataku jest **wyłudzenie poufnych danych**, takich jak dane logowania, dane osobowe lub finansowe, bądź nakłonienie użytkownika do kliknięcia w złośliwy link lub pobrania pliku zawierającego malware.

Przykładami takich wiadomości są:

- fałszywe potwierdzenia zamówień,
- wiadomości o rzekomym problemie z kontem,
- e-maile informujące o pilnej konieczności podjęcia działania.

Atak ten bazuje na nieuważności i presji czasu, aby zmanipulować użytkownika do podjęcia błędnej decyzji.

Platformy szkoleniowe

W celu zdobycia praktycznego doświadczenia wykorzystałam następujące platformy:

- **TryHackMe – SOC Simulator (Phishing scenario) [Korzystałam z wersji z platformą SPLUNK]**
  https://tryhackme.com/soc-sim/scenario-onboarding
    - → „Przykładowe analizy incydentów – phishing.pdf”
- **Public Summary – TryHackMe**
  https://tryhackme.com/soc-sim/public-summary/1687a5ae0e619feca1b61668ef1de80eb5e7267c4a8292486e3139131c3d38d6e5ed47be178c7863b17f55673ba34a6c
- **LetsDefend – Endpoint Analysis (krok po kroku)**
  https://app.letsdefend.io/training/lesson_detail/endpoint-analysis

Zdobyte potwierdzenie umiejętności (badge):
https://app.letsdefend.io/my-rewards/detail/a40a9fa0ce814bd58bdf7a9c9f8259ca

---

Proces analizy incydentu

1. Analiza wiadomości e-mail

- Zebranie podstawowych danych: nadawca, odbiorca, data, godzina, treść wiadomości
- Ocena podejrzanych linków i załączników
- Analiza nagłówków, domen i formatowania w celu wykrycia podszywania się pod legalne źródła

---

2. Analiza linków i załączników

Jeżeli wiadomość zawiera linki lub pliki, należy je zweryfikować przy użyciu narzędzi analitycznych, takich jak:

- **AnyRun** – interaktywna analiza malware (sandbox),
- **VirusTotal** – analiza plików i URL-i,
- **URLHaus** – baza złośliwych adresów URL,
- **URLScan** – skanowanie i analiza stron internetowych,
- **Hybrid Analysis** – analiza malware.

Pliki i linki powinny być analizowane wyłącznie w **bezpiecznym, izolowanym środowisku**.

---

3. Interakcja użytkownika

Jest to kluczowy element determinujący dalsze kroki eskalacji incydentu:

- czy użytkownik kliknął w link,
- czy pobrał lub uruchomił załącznik,
- czy udostępnił plik dalej.

Jeżeli użytkownik **nie podjął żadnej interakcji**, działania ograniczają się do:

- usunięcia e-maila,
- zablokowania adresu nadawcy i domeny,

Jeśli doszło do interakcji, konieczna jest dalsza analiza logów systemowych i sieciowych oraz eskalacja incydentu.

---

4. Analiza logów i ruchu sieciowego

Logi są kluczowym źródłem informacji pozwalającym określić **zakres (scope) incydentu**:

- podejrzane połączenia sieciowe,
- przesył danych do zewnętrznych hostów,
- adresy IP wykonujące nietypowe połączenia.

Do weryfikacji adresów IP można wykorzystać m.in.:

- **AbuseIPDB** – reputacja adresów IP.

---

5. Analiza endpointa

W przypadku podejrzenia infekcji należy przeanalizować:

- uruchomione procesy,
- aktywność hosta w sieci,
- historię terminala (podejrzane komendy),
- historię przeglądarki (złośliwe strony, pobrane pliki).

---

6. Reakcja na incydent

Szybkie działanie jest kluczowe. W przypadku potwierdzenia infekcji:

- host powinien zostać **natychmiast odłączony od sieci** – (izolacja),
- należy zapobiec dalszemu rozprzestrzenianiu się malware,
- zablokować złośliwe domeny/adresy,
- wdrożyć odpowiednie działania naprawcze i prewencyjne.

Dokumentacja i raportowanie incydentu

Każdy incydent w SOC wymaga pełnej dokumentacji – od pierwszego zgłoszenia, przez analizę, aż po wnioski i działania prewencyjne. W projekcie phishingowym dokumentacja obejmowała:

- Zbieranie faktów: data, godzina, nadawca, odbiorca, treść wiadomości, obecność linków i załączników
- Analizę narzędziami OSINT i sandbox (AnyRun, VirusTotal, URLScan, AbuseIPDB)

- Śledzenie interakcji użytkownika i wpływu na eskalację incydentu
- Analizę logów sieciowych i endpointowych, w tym podejrzanych procesów i transferów danych
- Rejestrację wszystkich kroków w postaci raportu, gotowego do przekazania zespołowi lub przełożonym

Dlaczego to ważne:

- Ułatwia odtworzenie przebiegu incydentu w razie audytu lub dalszej analizy
- Pozwala na przekazanie wiedzy innym członkom zespołu SOC
- Wspiera proces doskonalenia procedur i polityk bezpieczeństwa

---

Zakończenie i wnioski końcowe

- Phishing pozostaje skutecznym atakiem ze względu na manipulację użytkownikiem i zaufanie do pozornie legalnych wiadomości
- Analiza nagłówków, linków i załączników pozwala wcześnie wykryć próby podszywania się
- Interakcja użytkownika determinuje skalę incydentu i potrzebę dalszej analizy
- Kliknięcie w złośliwy link lub uruchomienie załącznika wymaga natychmiastowej analizy logów endpointa, ruchu sieciowego oraz potencjalnych połączeń C2 (Command and Control).
- Logi sieciowe i endpointowe pozwalają określić źródło i zakres incydentu
- Narzędzia OSINT (VirusTotal, AbuseIPDB) są skutecznym wsparciem
- Izolacja zainfekowanego hosta od sieci jest krytycznym działaniem ograniczającym rozprzestrzenianie się malware oraz dalszą eksfiltrację danych.
- Analiza procesów, historii terminala oraz aktywności przeglądarki pozwala na potwierdzenie lub wykluczenie obecności malware na hoście.
- Dokumentacja działań są kluczowe dla prawidłowego zarządzania incydentem oraz wdrożenia działań zapobiegawczych.