Relazione del Lavoro Svolto e Motivazione della Scelta dello Scenario

Introduzione

Il presente lavoro si concentra sull'analisi e simulazione di uno scenario di phishing relativo a un'email fraudolenta che simula una comunicazione ufficiale dal Tribunale di Polizia Municipale di Roma. Lo scenario è stato progettato per addestrare utenti e professionisti della sicurezza informatica a riconoscere tentativi di phishing e per sensibilizzare sull'importanza di adottare pratiche sicure nel trattamento delle email sospette.

Descrizione dello Scenario

Lo scenario ruota attorno a un tentativo di phishing mirato inviato a un individuo, Alfio Scuderi, sotto forma di un'email ufficiale che apparentemente proviene dal Tribunale di Polizia Municipale di Roma. Il contenuto dell'email richiede un'azione urgente da parte del destinatario, il quale deve confermare la propria partecipazione a un'udienza programmata entro 24 ore, accedendo a un link sospetto.

- **Oggetto dell'Email:** "Urgente: Azione Richiesta per la Tua Udienza presso il Tribunale di Polizia Municipale di Roma"
- **Corpo dell'Email:** Viene presentata una richiesta di conferma immediata dei dettagli dell'udienza per evitare conseguenze legali gravi. Il destinatario è invitato a cliccare su un link che porta a un sito web di phishing.
- **Obiettivo del Phishing:** Raccogliere informazioni personali e sensibili, come nome completo, indirizzo, dettagli bancari e altre informazioni utili a compiere frodi o furti d'identità.

Analisi dell'Email di Phishing

L'email presenta diversi elementi tipici dei tentativi di phishing, ma anche segnali che potrebbero far sorgere dubbi sulla sua legittimità:

- **Aspetti che Rendono l'Email Credibile:**
    1. **Aspetto Ufficiale:** L'email utilizza un linguaggio formale e appare come una comunicazione legale.
    2. **Richiesta Urgente:** Viene enfatizzata un'azione da compiere rapidamente, inducendo panico nel destinatario.
    3. **Dettagli Specifici:** Il riferimento a un'udienza e alle sue possibili conseguenze legali aumenta il livello di plausibilità.
- **Elementi di Allarme:**
    1. **Link Sospetto:** L'URL inserito non appartiene a un dominio ufficiale.
    2. **Richiesta di Informazioni Sensibili:** Un tribunale legittimo non richiederebbe la conferma di dettagli personali tramite un link esterno.
    3. **Dati di Contatto Non Verificabili:** Numero di telefono e indirizzo email non risultano facilmente confermabili attraverso canali ufficiali.

Motivazione della Scelta dello Scenario

Questo scenario è stato scelto per le seguenti motivazioni:

1. **Realismo:** Il phishing è una delle tecniche di attacco informatico più diffuse e il suo utilizzo è in continua crescita. La simulazione di un contesto legale con un'email apparentemente inviata da un'istituzione pubblica aumenta il realismo e la gravità percepita.
2. **Complessità dell'Attacco:** L'email è ben strutturata e sfrutta la psicologia dell'urgenza e della paura, aspetti comuni nei tentativi di phishing avanzati.
3. **Formazione degli Utenti:** Questo tipo di scenario è utile per sensibilizzare gli utenti a verificare sempre le fonti delle comunicazioni che ricevono e a non cliccare su link sospetti senza adeguate verifiche.
4. **Coinvolgimento di Autorità Legittime:** Attacchi che coinvolgono enti governativi o legali risultano particolarmente efficaci per i malintenzionati, poiché sfruttano il timore delle conseguenze legali.

Conclusioni

La simulazione del phishing relativo a un'udienza presso il Tribunale di Polizia Municipale di Roma è stata selezionata per le sue caratteristiche credibili e per la capacità di mettere in evidenza i rischi associati al phishing. Tale scenario è particolarmente utile per addestrare il personale a riconoscere i segnali di un attacco di phishing, prevenendo il furto di informazioni personali e migliorando la sicurezza informatica complessiva.