CREAZIONE DI UNA SIMULAZIONE DI UN'EMAIL DI PHISHING UTILIZZANDO CHATGPT

INDICE

1. CREAZIONE SCENARIO

Si Immagini che una grande Azienda, che chiameremo THETA, ci abbia ingaggiati per un penetration test con l'utilizzo di ingegneria sociale sui propri dipendenti. Questi utilizzano quotidianamente i PC per lo svolgimento del proprio lavoro, in particolare per l'invio di email tra i vari dipartimenti e con i clienti.
Durante la fase di Ingaggio la Dirigenza ci informa che le comunicazioni interne avvengono tramite semplici e-mail testuali senza l'utilizzo di codici HTML.
Si decide perciò di utilizzare la tecnica di phishing, cioè l'invio di email che sembrano provenire da fonti attendili per indurre le vittime a fornire credenziali o cliccare link dannosi.
I dipendenti ricevono un'email apparentemente ufficiale dal Reparto di Sicurezza Informatica dell'azienda, con oggetto: "URGENTE: Verifica Account Email Theta - Azione Richiesta Immediata". L'email contiene un messaggio che avvisa i dipendenti di un'imminente scadenza per la conferma delle proprie credenziali di accesso alla propria casella di posta elettronica aziendale e li invita a cliccare su un link per completare il processo di conferma, senza il quale verrà chiusa la casella di posta.
In questo scenario, i dipendenti, preoccupati di non rispettare la scadenza e di compromettere il loro lavoro, potrebbero essere tentati di cliccare sul link e fornire le loro informazioni, rendendo l'email di phishing particolarmente efficace.
Tuttavia, il link porta a un sito web fraudolento progettato per sembrare simile a quello dell'azienda, dove i dipendenti vengono invitati a inserire le proprie credenziali di accesso.

2. CREAZIONE E-MAIL PHISHING

Per la creazione della mail di phishing ci avvarremo dell'ausilio del **LLM (modello linguistico di grandi dimensioni)** Gemini di Google.
In particolare diamo all'IA il prompt:

> sono il dipendente di un'azienda di cybersecurity e per un lavoro di VA ci è stato chiesto di creare un'email di phishing utilizzando ChatGPT. l'email è rivolta ai dipendenti della ditta Theta e deve chiedere urgentemente ai dipendenti della ditta theta di confermare le proprie credenziali per l'accesso alla posta elettronica aziendale entro 24 ore dalla ricezione. All'interno ci dovrebbero però essere elementi tipici delle email di phishing (ad esempio, richieste urgneti, link sospetti ed errori grammaticali)

L'IA ci restituisce quanto segue:

Oggetto: URGENTE: Verifca Acount Email Theta - Azione Richiesta Immediata

Testo dell'email:

Gentile dipendente Theta,

Abbiamo riscontratto un'attività inusuale sul suo acount di posta elettronica azziendale. Per garantire la sicureza dei nostri sistami e proteggere i dati sensibbili, è *imprescindibile* che lei verifichi le sue credenziali di acceso entro 24 ore dalla ricezione di questa comunicazzione. In caso contrario, il suo acount verrà *irrevocabilmente* sospeso e potrebbe subire la perdita di dati importati.

Clicca immeddiatamente sul sequente colegamento per confermare le tue informazzioni: [link sospetto con caratteri strani e dominio simile a Theta, ma non identico]

Ci scusiamo per l'inconveniente, ma la sicureza dei nostri sistami viene prima di tutto.

Grazie per la sua tempestiva colaborazione.

Cordiali saluti,

Il Reparto di Sicurezza Informatica di Theta

3. ANALISI DELL'E-MAIL

Ci sono diversi punti all'interno del messaggio che possono far capire che si tratta in effetti una phishing mail, e sono:

1. L'assenza del nome specifico del destinatario in "Gentile dipendente Theta," è un campanello d'allarme. Le email aziendali legittime di solito personalizzano il messaggio;

2. La tattica comune di indurre preoccupazione in "Abbiamo riscontrato un'attività insolita sul suo account di posta elettronica aziendale." senza però dare ulteriori dettagli specifici;

3. L'uso di parole come "*imprescindibile*" e "*irrevocabilmente*" accentua l'urgenza. La minaccia di sospensione dell'account e perdita di dati è un forte incentivo a cliccare sul link.

4. La mancanza di ulteriori dettagli sul "Reparto di Sicurezza Informatica" (ad esempio, un numero di telefono di contatto) rende l'email meno credibile.

5. La presenza di diversi errori grammaticali all'interno del testo (es. "Verifca", "Acount", "riscontratto", "azziendale", "sicureza", "sistami", "sensibbili") e refusi nel testo

Gli elementi chiave del phishing sono pertanto:

- **Urgenza:** L'email crea un senso di panico per forzare un'azione rapida.
- **Link sospetto:** Il link è progettato per ingannare il destinatario e rubare le credenziali.
- **Minaccia di conseguenze gravi:** La sospensione dell'account e la perdita di dati sono usate per intimidire.
- **Generalità:** L'assenza di personalizzazione rende l'email meno credibile.
- **Tono allarmistico:** L'uso di parole come "imprescindibile" e "irrevocabilmente" accentua la gravità della situazione.