Social Engineering

In seguito all'implemento delle IA nel nostro quotidiano, la richiesta è stata quella di recuperare informazioni sull'ingegneria sociale, cos'è, come viene utilizzata, e come difendersi.

Quando un possibile attaccante, solitamente un black hat, decide di sviluppare un attacco verso una rete, si troverà di fronte a due strade. Ci sarà chi preferisce l'approccio informatico, estrapolando informazioni fino a risalire all'indirizzo IP della vittima per poi iniziare a muoversi nella rete, alla ricerca di dati sensibili, e chi preferisce un approccio differente, adoperando l'ingegneria sociale.

Cos'è però l'ingegneria sociale?

L'ingegneria sociale, o **social engineering** è una tecnica di manipolazione psicologica utilizzata per indurre le persone a rivelare informazioni riservate, effettuare azioni dannose o violare le proprie difese di sicurezza. A differenza degli attacchi informatici che si concentrano sulle vulnerabilità tecnologiche, il social engineering sfrutta le debolezze umane – come la fiducia, la curiosità, la paura o l'urgenza – per ottenere accesso a dati sensibili o compiere truffe. Le tecniche principali utilizzate da chi lo pratica sono:

- **Phishing** – probabilmente la più diffusa. Questa tecnica consiste nell'invio di email, messaggi di testo o comunicazioni che sembrano provenire da fonti affidabili e che contengono un link o un allegato dannoso, il cui scopo è quello di indurre l'utente a cliccare sul link.
- **Spear phishing** – si tratta di un attacco phishing più mirato, dove l'attaccante prende di mira un individuo specifico o un gruppo ristretto utilizzando informazioni personali o professionali per rendere l'attacco più credibile.
- **Whaling –** consiste in un attacco phishing mirato alle persone più importanti in un'azienda.
- **Vishing** – o voice phishing, consiste nell'uso di chiamate telefoniche per fingersi operatori di banca, rappresentanti di servizi pubblici o altre figure autorevoli, utilizzando tecniche di persuasione al fine di rivelare informazioni riservate.
- **Deepfake Voice Attack** - una tecnica relativamente recente che sfrutta l'intelligenza artificiale per creare imitazioni vocali realistiche di una persona. L'attaccante può usare una voce sintetizzata per impersonare un collega o un superiore e indurre la vittima a rivelare informazioni sensibili o a compiere azioni.
- **Baiting** - consiste nel "adescare" la vittima con una promessa allettante. Un esempio comune è l'inserimento di una chiavetta USB infetta in un luogo strategico, sperando che qualcuno la prenda e la inserisca nel proprio computer. Quando verrà aperta il malware sarà installato in automatico.
- **Pretexting** - con questa tecnica, l'attaccante costruisce una storia credibile (o *pretesto*) per giustificare la richiesta di informazioni. Ad esempio, può fingere di essere un tecnico IT che ha bisogno delle credenziali di accesso per risolvere un problema, oppure un rappresentante di un'autorità legale che richiede dati confidenziali per un'indagine.
- **Impersonation -** gli attaccanti, in questo caso, si fingono qualcun altro, come un collega o un cliente. Spesso questo avviene fisicamente, ad esempio introducendosi in un edificio riservato, oppure attraverso comunicazioni digitali, molto efficace se utilizzata insieme al Pretexting.
- **Shoulder surfing -** Consiste nell'osservare la vittima mentre inserisce password o codici di accesso, senza che quest'ultima se ne accorga.
- **Honeytrap -** L'attaccante si finge interessato romanticamente alla vittima per creare una relazione di fiducia e convincerla a rivelare informazioni private o aziendali.
- **Watering Hole Attack -** In questo caso, gli hacker identificano siti web che il target frequenta abitualmente e li compromettono con malware. Quando la vittima visita questi siti, il suo dispositivo viene infettato, permettendo agli attaccanti di accedere ai suoi dati o alla rete aziendale a cui è collegato.

Come difendersi da queste innumerevoli minacce?

Al giorno d'oggi essere i bersagli di attacchi di ingegneria sociale è purtroppo molto comune, una semplice mail può rivelarsi molto pericolosa e causare danni irreparabili, ma vi sono alcune accortezze e delle ottime pratiche che possono aiutare a prevenire e difendersi da questi attacchi.

- **Educazione e consapevolezza** – esse sono alla base di tutto, dipendenti e gli utenti devono essere formati per riconoscere i tentativi di social engineering e sapere come agire. Ottimale sarebbe istruirli in modo specifico nel riconoscere possibili email di phishing, mettendo loro a conoscenza di 3 parametri fondamentali per il controllo di una possibile mail dannosa, **SPF**, **DKIM**, e **DMARC**.
- **Verifica dell'identità** - Non fidarsi immediatamente di chiamate, email o messaggi non richiesti. È sempre meglio confermare l'identità dell'interlocutore tramite canali indipendenti (come una seconda chiamata al numero ufficiale dell'azienda).
- **Autenticazione a più fattori (MFA)** - Anche se le credenziali vengono rubate, l'MFA aggiunge un ulteriore livello di sicurezza per proteggere gli account.
- **Non condividere informazioni sensibili** - Le informazioni personali o aziendali dovrebbero essere condivise solo se strettamente necessario, e con persone di cui si ha piena fiducia.
- **Verifica dei link e degli allegati** - Prima di cliccare su link o aprire allegati, è importante controllare che siano sicuri, ad esempio passando il cursore sul link per vedere l'URL o esaminando attentamente l'indirizzo email del mittente. Controllare al presenza di possibili errori grammaticali, incongruenze con email ricevute precedentemente riguardanti il medesimo servizio, e controllare i 3 fattori sopra citati.

La tutela delle informazioni riservate è essenziale, poiché la perdita, furto o divulgazione di esse è senza prezzo, e può causare danni irreparabili al punto da poter portare un'azienda a chiudere i battenti.

Queste preoccupazioni sono però rivolte anche ai singoli, che navigano quotidianamente nel web, noi tutti potremmo essere scelti in futuro per un attacco di social engineering. Per cui ulteriori raccomandazioni possono essere scegliere password sicure, cambiarle con frequenza, e fare attenzione a possibili mail di phishing, esempi molto importanti per la prevenzione di attacchi di social engineering, e la salvaguardia delle nostre informazioni.