Social Engineering e Tecniche Comuni Utilizzate dagli Attaccanti

Il social engineering è una tecnica di manipolazione psicologica utilizzata da malintenzionati per ingannare le persone e convincerle a rivelare informazioni riservate o a compiere azioni che potrebbero compromettere la sicurezza di un’organizzazione o di un individuo. A differenza di altri tipi di attacchi che sfruttano vulnerabilità tecniche, il social engineering si basa sull’inganno, sulla fiducia e sulla manipolazione delle persone, spesso facendole agire contro il loro stesso interesse.

# Tecniche Comuni di Social Engineering

# Phishing

Il phishing è una delle tecniche più diffuse di social engineering. Gli attaccanti inviano email, messaggi di testo o creano siti web che sembrano provenire da fonti affidabili, come banche, servizi online o colleghi di lavoro. Questi messaggi sono progettati per indurre la vittima a cliccare su un link, scaricare un allegato o fornire informazioni sensibili, come credenziali di accesso o dati finanziari.

Esempio: Un'email che sembra provenire dalla tua banca, che ti chiede di aggiornare le tue credenziali per evitare la sospensione del conto.

# Pretexting

Il pretexting è una tecnica in cui l'attaccante crea un pretesto o una storia convincente per ottenere informazioni personali dalla vittima. Questo pretesto potrebbe coinvolgere la creazione di un'identità fittizia o l'imitazione di un'autorità (come un agente di polizia, un dirigente aziendale, o un tecnico IT).

Esempio: Un finto tecnico IT che chiama un dipendente affermando di dover risolvere un problema urgente e richiede le credenziali di accesso al sistema.

# Baiting

Il baiting implica l'offerta di un’esca per attirare la vittima a compiere un'azione dannosa. L’esca può essere un dispositivo fisico (come una chiavetta USB infetta) o un'offerta allettante online, come il download gratuito di un film o un software.

Esempio: Una chiavetta USB 'perduta' con un'etichetta accattivante come 'Rapporto salariale 2024' lasciata in un luogo visibile. La vittima la raccoglie e la inserisce nel proprio computer, infettandolo con malware.

# Tailgating

Il tailgating, noto anche come piggybacking, è una tecnica in cui un attaccante entra in un'area sicura seguendo da vicino una persona autorizzata. Questo tipo di attacco sfrutta la cortesia o la distrazione della vittima, che può tenere aperta una porta per qualcuno che sembra un collega o un visitatore legittimo.

Esempio: Un individuo senza badge segue un dipendente in un edificio sicuro affermando di aver dimenticato il proprio badge.

# **Vishing (Voice Phishing)**

Il vishing è una variante del phishing che utilizza le chiamate vocali per ingannare le vittime. Gli attaccanti si spacciano per entità legittime, come istituti bancari o rappresentanti di servizi, e convincono le vittime a fornire informazioni personali o finanziarie.

Esempio: Una telefonata da qualcuno che si spaccia per un rappresentante della tua banca, che ti informa di un'attività sospetta sul tuo conto e ti chiede di confermare i dettagli del tuo conto o la tua password.

# Deepfake Voice Attacks

Questo tipo di attacco sfrutta la tecnologia dei deepfake per creare registrazioni audio realistiche che imitano la voce di una persona specifica. Gli attaccanti usano queste registrazioni per convincere le vittime a compiere azioni o rilasciare informazioni sensibili, credendo di parlare con una persona di fiducia.

Esempio: Un dirigente di un'azienda riceve una telefonata che sembra provenire dal CEO, con una voce identica a quella del vero CEO, che richiede un trasferimento urgente di fondi.

Strategie di Difesa contro gli Attacchi di Social Engineering

# Phishing

* Formazione continua: I dipendenti e gli utenti devono essere istruiti regolarmente per riconoscere i segnali di phishing, come URL sospetti, errori grammaticali e richieste di informazioni personali.
* Utilizzo di filtri anti-phishing: I software di sicurezza possono bloccare messaggi sospetti prima che raggiungano la posta in arrivo.
* Autenticazione a due fattori (2FA): Implementare il 2FA come ulteriore livello di protezione anche nel caso in cui una password venga compromessa.

# Pretexting

* Verifica dell'identità: Richiedere sempre conferme indipendenti dell'identità di chi richiede informazioni sensibili.
* Politiche aziendali: Le aziende devono stabilire e applicare rigorosi protocolli per la divulgazione di informazioni riservate, soprattutto per via telefonica o tramite e-mail.

# Baiting

* Educazione sulla sicurezza: Formare gli utenti a non inserire dispositivi sconosciuti nei loro computer e a non scaricare file da fonti sospette.
* Software di sicurezza aggiornato: Installare antivirus e programmi anti-malware aggiornati che possano rilevare eventuali minacce provenienti da dispositivi esterni o file scaricati.

# Tailgating

* Controllo degli accessi fisici: Implementare badge di sicurezza e tornelli o serrature a tempo che richiedono l'autenticazione di ogni persona che entra.
* Politiche di sicurezza fisica: I dipendenti devono essere istruiti a non consentire l'accesso ad aree protette a chi non ha un’autorizzazione esplicita.

# Vishing

* Formazione sulla sicurezza telefonica: Educare i dipendenti a non divulgare informazioni sensibili al telefono senza verificare l’identità del chiamante.
* Verifica delle richieste: Le aziende dovrebbero disporre di un processo per la verifica delle chiamate telefoniche, in cui i dipendenti richiedono ulteriori conferme per le richieste di informazioni confidenziali.

# Deepfake Voice Attacks

* Codici di verifica segreti: Implementare codici di sicurezza univoci che possono essere utilizzati per verificare l’identità nei casi di richieste telefoniche sospette.
* Software di rilevamento di deepfake: Utilizzare tecnologie avanzate che analizzano le caratteristiche vocali e possono rilevare le alterazioni da deepfake.