SOCIAL ENGINEERING E TECNICHE DI DIFESA

Il social engineering è una disciplina di attacco che si basa sulla manipolazione psicologica e sull'ingegneria del comportamento umano per compromettere la sicurezza informatica, aziendale o personale. A differenza delle tecniche di hacking tradizionali, che puntano a sfruttare vulnerabilità tecniche, il social engineering mira a sfruttare la fiducia, l'ignoranza o la disattenzione delle persone per aggirare le misure di sicurezza.
Gli attacchi di social engineering possono essere condotti in modo passivo, ad esempio tramite l'osservazione, o attivo, mediante interazione diretta con la vittima. Le tecniche più utilizzate possono variare in complessità e scalabilità, ma condividono l'obiettivo di ottenere accesso non autorizzato a informazioni, credenziali o risorse fisiche.

Tecniche comuni di social engineering

1. Phishing

Il phishing rappresenta una delle forme più diffuse di social engineering ed è realizzato principalmente tramite:
Email spoofing: invio di email con mittenti contraffatti per sembrare legittimi (es. banche, fornitori di servizi).
Link malevoli: URL manipolati per reindirizzare la vittima a siti falsi che raccolgono credenziali.
Payloads nascosti: allegati (PDF, DOCX, XLS) contenenti codice malevolo.
Caratteristiche avanzate: utilizzo di sottodomini realistici o domini simili (es. secure-login-bank.com anziché bank.com).
Messaggi personalizzati per colpire specifici reparti aziendali (es. fatture per l'amministrazione).

Mitigazione:
- Configurare autenticazioni multifattoriali (MFA).
- Applicare regole di sicurezza e filtri sui gateway email per bloccare domini malevoli.

2. Spear Phishing

Variante mirata del phishing, in cui l'attaccante utilizza informazioni contestuali raccolte tramite OSINT (Open Source Intelligence) o precedenti violazioni per rendere il messaggio altamente credibile.

Esempio:
Un attacco spear phishing indirizzato a un amministratore IT potrebbe includere riferimenti a sistemi specifici usati dall'azienda, come
"Aggiornamento critico richiesto per Cisco ISR 4331".

Mitigazione:
- Monitoraggio continuo per identificare account compromessi o attività anomale.
- Implementazione di politiche di Least Privilege Access.

3. Tailgating

Il tailgating (o piggybacking) è un attacco fisico in cui l'attaccante accede a un’area protetta sfruttando la mancata attenzione o la cortesia degli utenti autorizzati.
Tecniche comuni: scenario basato sull’urgenza: Un attaccante con un badge falso si avvicina alla porta mentre una persona autorizzata entra, chiedendo di essere fatto passare.
Stratagemma logistico: Portare oggetti voluminosi o pesanti per rendere più plausibile la richiesta di aiuto.

Mitigazione:
- Installazione di sistemi di controllo accessi con registrazione obbligatoria (badge personali con PIN o biometrici).
- Formazione sul rispetto delle policy di accesso.

4. Baiting

Il baiting sfrutta la curiosità o l’avidità della vittima per indurla a interagire con risorse compromesse, come file o dispositivi.

Esempio avanzato:
Un attaccante lascia una chiavetta USB con etichetta “Contratti riservati 2024” in un luogo strategico. Collegando la chiavetta, la vittima innesca malware progettati per eseguire exfiltration di dati.

Mitigazione:
-Disabilitare l’esecuzione automatica su dispositivi esterni.
-Implementare endpoint protection con funzioni di analisi comportamentale.

5. Pretexting

Il pretexting consiste nel creare uno scenario credibile (pretesto) per ottenere informazioni riservate. L'attaccante si presenta spesso come:

- Tecnico IT che richiede accesso al sistema.
- Addetto alle risorse umane che verifica dati personali.

Esempio:
Un attaccante si spaccia per un fornitore esterno e chiede dettagli sulle configurazioni di rete per "risolvere un problema tecnico".

Mitigazione:
- Verifica rigorosa delle identità tramite callback o autenticazione a più fattori.

- Applicazione di politiche di segregazione dei ruoli (SoD, Segregation of Duties).

6. Shoulder Surfing

Questa tecnica si basa sull'osservazione diretta del comportamento della vittima. Può essere condotta:

- Fisicamente, ad esempio guardando qualcuno inserire una password.
- Tramite l'uso di dispositivi ottici come telecamere nascoste.

Mitigazione:
- Utilizzo di filtri privacy per schermi.
- Politiche di clean desk per limitare l'esposizione di informazioni visibili.

7. Impersonation

L'attaccante assume l'identità di un individuo o un'entità autorizzata. Può utilizzare tecniche come:
Voice phishing (vishing): Telefonate in cui l'attaccante si presenta come supporto tecnico o autorità.
Deepfake audio/video: Per simulare dirigenti o colleghi.

Esempio: un attaccante utilizza una voce sintetizzata basata su AI per convincere un dipendente a effettuare un bonifico.

Mitigazione:
- Verifica indipendente delle richieste, specialmente in ambito finanziario.
- Integrazione di strumenti per rilevare deepfake.

8. Quid Pro Quo

Un attacco basato sull'offerta di un beneficio in cambio di informazioni o azioni specifiche. L'attaccante simula una situazione in cui l'utente crede di ricevere un vantaggio tangibile.

Esempio: un falso tecnico IT chiama un dipendente offrendo "supporto gratuito per migliorare le prestazioni del computer" e richiede le credenziali per accedere al dispositivo.

Mitigazione:
- Implementare politiche che richiedano verifiche ufficiali per qualsiasi offerta di assistenza tecnica.
- Educare i dipendenti a non fornire credenziali su richiesta.

10. Watering Hole

Gli attaccanti compromettono siti web popolari o specifici, sapendo che il target utilizza quei siti.
L'obiettivo è infettare gli utenti con malware quando visitano il sito compromesso.
Caratteristiche avanzate: attacchi mirati verso portali usati da settori specifici (es. siti di fornitori di tecnologia o formazione).
Inserimento di script malevoli in sezioni invisibili del sito (es. iframe nascosti).

Mitigazione:
- Utilizzo di DNS filtering per bloccare siti non sicuri.
- Implementazione di browser con sandboxing per ridurre i danni da exploit.

11. Smishing (SMS Phishing)

Simile al phishing, ma condotto tramite SMS o app di messaggistica (es. WhatsApp, Telegram). L'attaccante invia messaggi con link o richieste ingannevoli.

Esempio: un SMS che informa la vittima di un problema con un pagamento, includendo un link a una pagina che simula quella del proprio servizio bancario.

Mitigazione:
- Configurare blocchi su URL noti per il phishing tramite soluzioni mobile device management (MDM).
- Educare gli utenti a non cliccare su link in messaggi non richiesti.

12. Pretext Injection in Ticketing Systems

Gli attaccanti sfruttano sistemi di gestione dei ticket aziendali (come ServiceNow, Jira) per generare richieste false che richiedano interventi o informazioni da parte del personale IT.

Esempio: un attaccante crea un ticket che richiede il reset di una password per un account legittimo, utilizzando dettagli reali per aumentare la credibilità.

Mitigazione:
- Verifica manuale delle richieste di reset password.
- Abilitazione di log dettagliati per identificare tentativi di abuso del sistema di ticketing.

13. Diversion Theft (Frode da Diversione)

Questa tecnica sfrutta la logistica aziendale, dirottando consegne o processi. L'attaccante manipola il sistema per far consegnare materiali o documenti riservati a un luogo sotto il suo controllo.

Esempio: un attaccante si finge un corriere e modifica un ordine aziendale per ottenere componenti hardware sensibili.

Mitigazione:
- Verifica dei fornitori e conferma degli ordini tramite canali separati.
- Monitoraggio delle spedizioni critiche tramite tracciamento digitale.

14. Dumpster Diving (Scavenging)

Gli attaccanti cercano informazioni sensibili scartate in modo non sicuro (es. documenti non triturati, vecchi dispositivi di memoria).

Esempio: recupero di documenti cartacei da cestini aziendali, come stampe contenenti configurazioni di rete o credenziali.

Mitigazione:
- Utilizzo obbligatorio di trituratori per documenti sensibili.
- Smaltimento sicuro dei dispositivi IT tramite distruzione fisica o cancellazione sicura dei dati (wiping).

15. Rogue Access Points

Un attaccante configura un access point Wi-Fi con lo stesso nome di una rete legittima per intercettare connessioni. Questo permette il Man-in-the-Middle (MitM), consentendo di catturare credenziali o dati sensibili.

Esempio: configurazione di un access point "Corporate-WiFi" in una sala conferenze per spingere i dipendenti a collegarsi.

Mitigazione:
- Implementazione di WPA3 e autenticazione certificata (802.1X).
- Disabilitazione delle connessioni automatiche alle reti non salvate.

16. Pharming

Manipolazione del DNS o del file host locale della vittima per reindirizzare a siti fraudolenti, anche se la vittima inserisce correttamente l'URL.
Caratteristiche avanzate: l'attacco può coinvolgere il DNS aziendale o vulnerabilità nei router per propagarsi su più dispositivi.
Utilizzo di certificati TLS falsi per aumentare la fiducia.

Mitigazione:
- Configurare DNS convalidati tramite DNSSEC.
- Monitoraggio dei file host aziendali per modifiche non autorizzate.

17. Evil Twin Attack

Simile al Rogue Access Point, ma con un focus su reti Wi-Fi pubbliche o condivise. L'attaccante replica una rete legittima, come quella di un aeroporto o un caffè, inducendo gli utenti a connettersi.

Esempio: una rete denominata "Café Free Wi-Fi" intercetta il traffico non cifrato degli utenti per rubare credenziali.

Mitigazione:
- Utilizzo obbligatorio di VPN per tutte le connessioni aziendali su reti pubbliche.
- Disabilitazione del Wi-Fi quando non necessario.

18. Clone Phishing

Una variante avanzata del phishing, dove l'attaccante replica un'email legittima già ricevuta dalla vittima, sostituendo i link con versioni malevole.

Esempio: una vittima riceve un'email apparentemente da un collega con lo stesso contenuto di un'email reale ricevuta in precedenza, ma con link che portano a siti compromessi.

Mitigazione:
- Configurare strumenti di analisi comportamentale su email (es. Microsoft Defender, Proofpoint).
- Insegnare agli utenti a verificare link e mittenti sospetti.

19. Honeytrap

Un attaccante crea un legame emotivo o relazionale con la vittima (online o offline), inducendola a condividere informazioni o compiere azioni.

Esempio: creazione di profili falsi su LinkedIn o social media per interagire con dipendenti e ottenere informazioni interne.

Mitigazione:
- Sensibilizzare i dipendenti sull'importanza di non condividere informazioni aziendali sui social.
- Monitoraggio delle connessioni social dei dirigenti per rilevare anomalie.

20. Reverse Social Engineering

L'attaccante induce la vittima a contattarlo per ottenere aiuto, creando così un falso senso di fiducia.

Esempio: un attaccante compromette un dispositivo aziendale, mostra un messaggio di errore e fornisce un numero di supporto che porta direttamente a lui.

Mitigazione:
- Educare i dipendenti a utilizzare esclusivamente i canali ufficiali per richiedere supporto tecnico.
- Monitorare la presenza di messaggi anomali nei sistemi.