RICERCA

Il **social engineering** è una tecnica di attacco in cui i malintenzionati manipolano le persone per ottenere informazioni riservate o per indurle a compiere azioni dannose, come fornire credenziali, scaricare malware o concedere accessi non autorizzati. A differenza di altri tipi di attacchi che si basano su vulnerabilità tecniche, il social engineering sfrutta le vulnerabilità umane, come la fiducia, l'urgenza, o la curiosità.

Tecniche comuni di social engineering :

1. Phishing

- **Descrizione**: Consiste nell'invio di e-mail, messaggi di testo o altre comunicazioni che sembrano provenire da fonti affidabili, ma che in realtà mirano a indurre l'utente a compiere azioni specifiche (es. cliccare su un link, scaricare un file, o inserire credenziali su un sito fasullo).
- **Esempio**: Ricevi un'e-mail apparentemente da una banca che ti chiede di aggiornare i tuoi dati personali cliccando su un link che porta a un sito fake.
- **Varianti**:
- **Spear phishing**: Target mirati, spesso basati su informazioni personali raccolte in precedenza.
- **Whaling**: Phishing mirato a persone di alto livello in un'organizzazione (es. CEO, dirigenti).
- **Smishing**: Phishing tramite SMS.
- **Vishing**: Phishing tramite telefonate.

2. Tailgating

- **Descrizione**: Consiste nel seguire una persona autorizzata per accedere a un'area riservata senza avere le proprie credenziali.
- **Esempio**: Un attaccante con in mano una scatola pesante finge di essere un corriere e chiede a qualcuno di tenere aperta la porta per lui, accedendo così a un'area protetta.
- **Tecniche correlate**:
  - **Piggybacking**: Simile a tailgating, ma con il consenso (ingannato) di chi apre la porta.

3. Pretexting

- **Descrizione**: L'attaccante si costruisce un’identità falsa per guadagnare fiducia e ottenere informazioni riservate.
- **Esempio**: Un finto rappresentante dell’IT chiama un dipendente, chiedendo la password per risolvere un "problema tecnico urgente".

4. Baiting

- **Descrizione**: Utilizza un'esca per attirare le vittime, come un dispositivo USB infetto lasciato in un luogo pubblico o un link con una promessa allettante.
- **Esempio**: Un attaccante lascia una chiavetta USB con un'etichetta tipo "Buste paga 2024" in un parcheggio aziendale, sperando che qualcuno la inserisca nel proprio computer.

5. Quid Pro Quo

- **Descrizione**: L'attaccante promette un vantaggio in cambio di informazioni o azioni.
- **Esempio**: Una persona chiama fingendo di essere un tecnico, promettendo un aggiornamento gratuito in cambio delle credenziali.

6. Dumpster Diving

- **Descrizione**: Consiste nel cercare informazioni sensibili nei rifiuti (es. documenti cartacei, vecchi dispositivi, etc.).
- **Esempio**: Recuperare un manuale con le politiche aziendali per comprendere le misure di sicurezza.

Per difendersi efficacemente dagli attacchi di social engineering, è fondamentale adottare un mix di strategie tecniche, comportamentali e organizzative. Di seguito sono elencate le migliori:

1. Educazione e Consapevolezza

- **Formazione periodica:** Offrire corsi di formazione regolari per tutti i dipendenti sulle tecniche di social engineering, come phishing, baiting e tailgating.
- **Simulazioni di attacco:** Condurre test periodici di phishing simulato per misurare la prontezza del personale e migliorare le loro capacità di riconoscere le minacce.
- **Diffusione di casi reali:** Condividere esempi pratici di attacchi per aiutare i dipendenti a capire l'impatto di questi rischi.

2. Procedure e Politiche di Sicurezza

- **Autenticazione a più fattori (MFA):**
  - Riduce drasticamente il rischio derivante da credenziali compromesse.
  - Implementare MFA su tutte le applicazioni aziendali critiche.
- **Accesso basato sui privilegi minimi (Principle of Least Privilege):**
  - Consentire ai dipendenti di accedere solo alle risorse necessarie per il loro lavoro.
- **Verifica dell'identità:**
  - Stabilire protocolli chiari per verificare l'identità di chi richiede informazioni o accesso, sia internamente che esternamente.
  - Ad esempio, confermare le richieste di modifica di account o trasferimenti finanziari tramite una telefonata diretta.

3. Protezione contro il phishing

- **Email filtering avanzato:**
  - Implementare filtri per email che rilevino e blocchino automaticamente i messaggi sospetti.
- **Controllo URL e domini:**
  - Verificare attentamente i domini delle email e i link nei messaggi per rilevare variazioni sottili (es. “micros0ft.com” invece di “microsoft.com”).
- **Banner di avviso:**
  - Contrassegnare le email provenienti da fonti esterne con avvisi per sensibilizzare i destinatari.
- **Evita link diretti nelle email:**
  - Fornire URL noti e sicuri invece di cliccare su collegamenti nei messaggi.

4. Difesa contro il tailgating

- **Badge di accesso individuale:**
  - Ogni dipendente deve usare il proprio badge per entrare nei locali. Vietare l'accesso tramite “passaggi multipli” (piggybacking).
- **Guardie o sistemi di controllo:**
  - Installare tornelli o sistemi di controllo biometrici.
- **Politiche contro l’accesso non autorizzato:**
  - Insegnare ai dipendenti a segnalare chiunque tenti di entrare senza autorizzazione.

5. Protezione fisica

- **Chiavette USB sconosciute:**
  - Educare i dipendenti a non collegare dispositivi USB trovati o ricevuti senza verifica.
- **Distruzione di documenti:**
  - Adottare distruggidocumenti per eliminare informazioni sensibili.
- **Crittografia dei dispositivi:**
  - Assicurarsi che laptop, hard disk e chiavette USB aziendali siano crittografati per proteggere i dati in caso di furto.

6. Protezione delle chiamate e comunicazioni (Vishing)

- **Politica di verifica telefonica:**
  - Richiedere sempre conferme tramite altri canali (es. email aziendale) per qualsiasi richiesta ricevuta al telefono.
- **Numeri di supporto ufficiali:**
  - Fornire ai dipendenti un elenco di numeri verificati da contattare in caso di dubbi.

7. Strumenti tecnologici

- **Software antiphishing:**
  - Soluzioni che analizzano email e siti web in tempo reale per bloccare contenuti fraudolenti.
- **Monitoraggio della rete:**
  - Strumenti di rilevamento delle intrusioni (IDS/IPS) che segnalano comportamenti anomali.
- **Sandboxing:**
  - Testare file sospetti in un ambiente isolato prima di aprirli o distribuirli.

8. Segnalazione e Gestione degli Incidenti

- **Creare una cultura della segnalazione:**
  - Incoraggiare i dipendenti a segnalare immediatamente comportamenti sospetti senza timore di ripercussioni.
- **Team di risposta agli incidenti:**
  - Avere un team dedicato per gestire segnalazioni e indagare su possibili attacchi.

Checklist per i Dipendenti

1. **Non cliccare su link sospetti.**
2. **Non condividere mai informazioni sensibili senza verifica.**
3. **Non lasciare porte o dispositivi incustoditi.**
4. **Segnalare subito comportamenti sospetti o richieste insolite.**
5. **Usare password complesse e cambiarle regolarmente.**