

Social Engineering e Tecniche di Difesa

Prompt utilizzato su chatgpt:

“Descrivi cos'è il social engineering e quali sono le tecniche più utilizzate dagli attaccanti? ho bisogno di una ricerca approfondita sui metodi e su come funzionano”

Risposta al prompt:

Cos'è il Social Engineering?

L'ingegneria sociale si basa sulla manipolazione della fiducia, della curiosità o della paura. Gli attaccanti non cercano di forzare i sistemi tecnologici, ma cercano di indurre una vittima a fornirgli volontariamente l'accesso o le informazioni. Questi attacchi possono avvenire online, via telefono, o di persona.

Obiettivi comuni:

- Credenziali (username e password)
 - Informazioni personali (dati bancari, numeri di carta di credito)
 - Accesso a sistemi aziendali
 - Installazione di malware
 - Compromissione di identità o ruoli
-

Tecniche più utilizzate nel Social Engineering

1. Phishing

Definizione: Invio di messaggi falsi (email, SMS, social media) che imitano comunicazioni ufficiali per indurre la vittima a cliccare su link malevoli o fornire dati personali.

Varianti:

- **Spear Phishing:** Mirato a un individuo specifico, spesso con dettagli personalizzati.
- **Whaling:** Targeting di figure di alto profilo (es. CEO, CFO).
- **Smishing:** Phishing via SMS.
- **Vishing:** Phishing via chiamate vocali.

Esempio: Un'email che sembra provenire dalla tua banca ti chiede di "verificare il tuo account" tramite un link falso.

2. Pretexting

Definizione: L'attaccante crea un pretesto credibile per ottenere informazioni dalla vittima. Si finge ad esempio un tecnico IT, un rappresentante della banca o un collega.

Come funziona:

- Si crea una storia credibile per legittimare la richiesta di dati.
- Si sfruttano dettagli pubblici (LinkedIn, social) per sembrare autentici.

Esempio: Una telefonata da parte di un falso tecnico che chiede le credenziali per "aggiornare il sistema".

3. Baiting

Definizione: Si offre qualcosa di gratuito o allettante (musica, software, premi) per indurre la vittima a scaricare malware o rivelare dati.

Esempio: Una chiavetta USB infetta lasciata in un luogo pubblico con un'etichetta "Contabilità 2025" – chi la inserisce nel PC esegue inconsapevolmente un malware.

4. Quid Pro Quo

Definizione: L'attaccante offre un beneficio in cambio di informazioni o accesso.

Esempio: Falsi operatori IT offrono supporto tecnico gratuito in cambio di accesso remoto al computer.

5. Tailgating (Piggybacking)

Definizione: Tecnica fisica in cui l'attaccante entra in un edificio protetto seguendo da vicino un dipendente legittimo.

Esempio: Un individuo con abbigliamento da corriere segue un impiegato in azienda senza badge.

6. Dumpster Diving

Definizione: L'attaccante cerca informazioni nei rifiuti (cartacei o elettronici) di aziende o individui.

Obiettivi: Appunti con password, documenti riservati, dispositivi smaltiti impropriamente.

Come Funzionano gli Attacchi di Social Engineering?

Fasi tipiche:

1. **Ricognizione (Reconnaissance):** Raccolta di informazioni pubbliche (social media, siti web, registri).
2. **Costruzione del rapporto:** L'attaccante stabilisce un contatto e una relazione di fiducia.
3. **Manipolazione:** Spinge la vittima ad agire come desiderato (cliccare, inviare info, aprire accesso).
4. **Esecuzione:** L'attaccante ottiene l'accesso o i dati desiderati.
5. **Copertura:** L'attaccante cancella le tracce o approfitta dell'accesso ottenuto.

Come ci si difende dal Social Engineering?

Prompt utilizzato su chatgpt:

“Mi specifichi in maniera completa le tecniche per difendersi da questi attacchi (dammi le migliori tecniche difensive per ogni tecnica di attacco)”

Risposta al prompt:

1. Phishing (inclusi spear phishing, whaling, smishing, vishing)

Tecniche Difensive:

- **Formazione continua del personale**
 - Simulazioni di phishing periodiche per allenare la reazione dei dipendenti.
 - Educazione al riconoscimento di email sospette (URL strani, errori grammaticali, urgenze sospette).
- **Filtro antispam e antiphishing avanzato**
 - Utilizzo di soluzioni come Microsoft Defender, Proofpoint, Barracuda o Google Workspace Security.
- **Autenticazione a più fattori (2FA/MFA)**
 - Anche se le credenziali vengono rubate, l'accesso è bloccato senza il secondo fattore.
- **Protezione DNS e filtraggio web**
 - Bloccare l'accesso a domini di phishing conosciuti.
- **Segnalazione interna semplice ed efficace**
 - Sistema per permettere ai dipendenti di segnalare

email sospette facilmente.

2. Pretexting (pretesto ingannevole per ottenere info o accesso)

Tecniche Difensive:

- **Verifica dell'identità per richieste sensibili**
 - Obbligo di conferma via canali separati (es. telefonata diretta al numero ufficiale del collega).
 - **Formazione su inganni comuni e casi reali**
 - Mostrare esempi di pretexting reali (CEO fraud, finti tecnici IT, falsi fornitori).
 - **Procedure rigide per il rilascio di informazioni**
 - Mai fornire dati sensibili su richiesta telefonica o email senza verifiche multilivello.
 - **Segmentazione e minimizzazione dei privilegi**
 - Solo chi ha realmente bisogno accede a dati sensibili (principio del minimo privilegio).
-

3. Baiting (esche fisiche o digitali con malware)

Tecniche Difensive:

- **Politica aziendale sul divieto di utilizzo di dispositivi esterni non autorizzati**
 - USB disabilitate o accesso limitato.

- **Blocco automatico dell'esecuzione da dispositivi rimovibili**
 - Configurazione dei sistemi per bloccare l'autorun da USB/CD/DVD.
 - **Formazione su comportamenti sospetti (es. chiavette trovate)**
 - Mostrare casi reali e statistiche sui rischi.
 - **Soluzioni EDR/antivirus avanzati**
 - Monitoraggio in tempo reale dell'esecuzione di software malevoli anche da supporti fisici.
-

4. Quid Pro Quo (scambio di favori in cambio di info o accesso)

Tecniche Difensive:

- **Politica: nessun supporto tecnico non richiesto è legittimo**
 - I dipendenti devono sapere che il supporto tecnico non contatta mai "a caso".
- **Autenticazione forte dei fornitori e degli operatori esterni**
 - Accessi a sistemi devono essere sempre approvati formalmente.
- **Formazione: diffidare dalle richieste d'aiuto o promesse sospette**
 - Ad esempio: "Ti do un buono Amazon se mi fai accedere a questo server..."

5. Tailgating / Piggybacking (accesso fisico non autorizzato)

Tecniche Difensive:

- **Badge identificativi obbligatori e visibili**
 - Badge diversi per visitatori, esterni, dipendenti.
- **Tornelli con accesso singolo**
 - Accesso controllato uno per volta con badge o riconoscimento biometrico.
- **Cultura della sicurezza fisica ("Security Awareness")**
 - I dipendenti devono sentirsi legittimati a bloccare chi non ha badge o a segnalarlo.
- **Videosorveglianza e controllo accessi registrato**
 - Registra entrate e uscite in tempo reale.

6. Dumpster Diving (raccolta info dai rifiuti)

Tecniche Difensive:

- **Distruzione sicura dei documenti**
 - Utilizzo di trita-documenti (livello di sicurezza P-4 o superiore) o servizio di distruzione certificato.
- **Smaltimento sicuro di dispositivi elettronici**
 - Cancellazione sicura dei dati (es. software di wiping,

degausser per dischi magnetici).

- **Cestini interni separati per documenti sensibili**
 - Differenziare i rifiuti “confidenziali” da quelli ordinari.