IL SOCIAL ENGINEERING

Il **social engineering** è una tecnica di manipolazione psicologica utilizzata per indurre le persone a rivelare informazioni riservate o a compiere azioni che violano le regole di sicurezza. Gli attaccanti si basano sull'inganno per sfruttare la fiducia, l'ingenuità o le emozioni delle vittime. Questa strategia è spesso usata per accedere a sistemi informatici, reti aziendali o informazioni sensibili senza dover affrontare meccanismi tecnici complessi.

Tecniche più comuni di social engineering:

1. Phishing

Gli attaccanti inviano email, messaggi o link che sembrano provenire da fonti affidabili (ad esempio banche, aziende, o colleghi di lavoro) con l'obiettivo di rubare credenziali, informazioni personali o indurre la vittima a compiere azioni specifiche, come scaricare malware.

- **Esempi**:
    - Email di "reset della password" fasulle.
    - Falsi messaggi di allarme (ad esempio: "Il tuo conto sarà bloccato!").
    - Offerte troppo belle per essere vere (ad esempio, vincite improvvise).

2. Spear phishing

Una versione mirata del phishing, in cui l'attaccante personalizza il messaggio in base alla vittima, utilizzando informazioni specifiche (spesso raccolte da social media o altre fonti).

- **Esempi**:
    - Un'email che sembra provenire dal CEO di un'azienda chiedendo un bonifico urgente.

3. Tailgating (o piggybacking)

L'attaccante si infiltra in un'area riservata seguendo fisicamente una persona autorizzata, sfruttando la cortesia o la distrazione.

- **Esempi**:
    - Seguire qualcuno attraverso una porta di sicurezza che richiede badge, facendo finta di averlo dimenticato.
    - Portare con sé oggetti (come un pacco) per giustificare la sua presenza.

4. Pretexting

Gli attaccanti creano una falsa identità o scenario per ingannare le vittime e convincerle a fornire informazioni o accesso.

- **Esempi**:
    - Fingere di essere un tecnico IT che necessita di informazioni di accesso.

    - Spacciarsi per un funzionario bancario per ottenere dati finanziari.

5. Baiting

L'attaccante attira la vittima offrendo qualcosa di desiderabile per indurla a compiere azioni che compromettano la sicurezza.

- **Esempi**:
    - Chiavette USB infette lasciate in luoghi pubblici con etichette accattivanti (ad esempio, "Documenti riservati").
    - Pubblicità fasulle che invitano a scaricare software dannosi.

6. Voice phishing (Vishing)

Versione del phishing tramite telefono, in cui l'attaccante si spaccia per una figura autorevole o fidata per ingannare la vittima.

- **Esempi**:
    - Telefonate che simulano supporto tecnico o richieste bancarie.

7. Shoulder surfing

L'attaccante osserva fisicamente la vittima mentre inserisce informazioni sensibili, come password o codici PIN.

- **Esempi**:
    - Spiare il PIN di una carta di credito in un bancomat.
    - Guardare qualcuno mentre digita la password su un computer.

Come proteggersi:

- **Verificare sempre le fonti** prima di cliccare su link o condividere informazioni.
- **Non fidarsi di richieste urgenti**: l'urgenza è spesso un segnale di manipolazione.
- **Bloccare l'accesso non autorizzato**: non consentire l'accesso a chiunque senza identificazione adeguata.
- **Abilitare l’autenticazione a due fattori** (2FA).
- **Formazione del personale**: educare sulle minacce di social engineering e su come riconoscerle.

Queste tecniche dimostrano quanto sia importante adottare comportamenti prudenti e mantenere un livello elevato di consapevolezza sulla sicurezza.

Formazione e Consapevolezza

Gli attacchi di social engineering si basano principalmente sull'ingenuità o sulla mancanza di conoscenza delle vittime.

- **Strategie**:
    - Organizzare regolari **corsi di formazione sulla sicurezza informatica** per dipendenti e utenti.
    - Simulare attacchi (es. phishing test) per insegnare a riconoscerli.
    - Sensibilizzare sull'importanza di **non condividere informazioni sensibili** con persone non autorizzate.

---

2. Applicare il principio del dubbio

Fidarsi è bene, verificare è meglio. Gli attacchi spesso si presentano sotto forma di richieste urgenti o provenienti da figure apparentemente autorevoli.

- **Strategie**:
    - **Verificare sempre l'identità** di chi chiede informazioni riservate, soprattutto se lo fa tramite email o telefono.
    - Non fidarsi di richieste che sembrano sospette o inusuali, anche se provenienti da colleghi o superiori.

---

3. Protezioni tecniche

La tecnologia può aiutare a identificare e bloccare gli attacchi.

- **Strategie**:
    - **Filtri antispam e antivirus aggiornati** per rilevare email o file malevoli.
    - Implementare strumenti di **autenticazione a due fattori (2FA)**, che rendono più difficile accedere ai sistemi anche se le credenziali vengono rubate.
    - Monitorare il traffico di rete per individuare attività anomale.

---

4. Politiche di sicurezza aziendale

Procedure chiare riducono il rischio di errori umani.

- **Strategie**:
    - Definire e comunicare regole aziendali per la condivisione di dati sensibili (ad esempio, mai tramite email o telefono senza una verifica aggiuntiva).
    - Implementare il principio del **minimo privilegio**: ogni dipendente dovrebbe avere accesso solo alle informazioni necessarie per il proprio lavoro.

    - Richiedere approvazioni formali per azioni critiche come bonifici bancari o modifiche dei dati degli utenti.

5. Difese fisiche

Gli attacchi di tipo tailgating o shoulder surfing sfruttano vulnerabilità fisiche o disattenzione della vittima.

- **Strategie**:
    - Utilizzare badge identificativi e controlli di accesso per limitare l'ingresso in aree riservate.
    - Installare videocamere di sorveglianza nelle zone sensibili.
    - Educare i dipendenti a non lasciare incustoditi documenti riservati o dispositivi come laptop.

---

6. Protezione delle informazioni personali

Gli attaccanti spesso raccolgono informazioni su vittime potenziali tramite social media o altre fonti pubbliche.

- **Strategie**:
    - Limitare le informazioni condivise pubblicamente sui social media.
    - Usare impostazioni di privacy per controllare chi può visualizzare i propri post o dettagli personali.
    - Prestare attenzione alle richieste di amicizia o connessioni sospette.

---

7. Segnalare attività sospette

Il feedback rapido e la comunicazione possono prevenire attacchi su larga scala.

- **Strategie**:
    - Creare un canale interno per **segnalare tentativi di social engineering** (es. email di phishing o telefonate sospette).
    - Incoraggiare una cultura aziendale in cui i dipendenti non temano di riferire situazioni ambigue.

---

8. Simulazioni di attacco

Mettere alla prova i propri sistemi e dipendenti aiuta a identificare debolezze.

- **Strategie**:
    - Eseguire test periodici di phishing per valutare la preparazione.
    - Simulare situazioni di tailgating o pretexting per vedere come le persone rispondono.

---

9. Usare l'intelligenza artificiale e strumenti di sicurezza avanzati

Strumenti AI **possono** rilevare modelli sospetti in e-mail o comportamenti degli utenti.

- **Strategie**:
    - Implementare sistemi di analisi delle minacce basati sull'intelligenza artificiale.
    - Usare strumenti di protezione endpoint per monitorare e bloccare attività sospette.

---

10. Mentalità zero-trust

Nessun accesso è dato per scontato, ogni richiesta deve essere verificata.

- **Strategie**:
    - Adottare il modello **Zero Trust** in cui tutte le identità, sia interne che esterne, sono continuamente validate.
    - Utilizzare sessioni temporanee o accesso condizionato per attività sensibili.

Seguendo queste strategie, individui e organizzazioni possono ridurre significativamente la probabilità di cadere vittime di attacchi di social engineering e aumentare la resilienza complessiva contro le minacce informatiche.Inizio modulo