1. Cos'è il Social Engineering?

Il **social engineering** è una forma di attacco che non si basa su vulnerabilità tecnologiche, ma su debolezze umane. Gli attaccanti manipolano psicologicamente le persone per ottenere informazioni riservate o accessi non autorizzati.

In pratica, invece di cercare di "bucare" un sistema con strumenti informatici, cercano di convincere le persone ad aiutarli involontariamente.

2. Tecniche comuni di Social Engineering

a. Phishing

- Una delle tecniche più utilizzate.
- Consiste nell'invio di e-mail o messaggi che sembrano provenire da una fonte affidabile (come una banca o un'azienda) per indurre la vittima a fornire informazioni sensibili.
- Tipi di phishing:
    - **E-mail phishing**: Finti messaggi e-mail che chiedono di inserire credenziali o scaricare allegati.
    - **Spear phishing**: Attacchi mirati, con messaggi personalizzati per una persona specifica.
    - **Smishing**: Phishing via SMS.

b. Tailgating

- In questo caso, l'attaccante segue fisicamente una persona autorizzata per accedere a un'area protetta senza avere il permesso.
- Esempio: Qualcuno si avvicina a una porta aziendale e si infiltra dietro un dipendente che apre la porta con il badge.

c. Pretexting

- Gli attaccanti creano una falsa identità o pretesto per ingannare la vittima.
- Potrebbero fingere di essere un tecnico IT o un rappresentante della banca per convincere la vittima a rivelare dati personali.

d. Baiting

- Questa tecnica sfrutta la curiosità umana.

- Gli attaccanti lasciano oggetti come chiavette USB in luoghi pubblici, sperando che qualcuno le raccolga e le inserisca nel proprio computer, attivando malware.

e. Vishing (Phishing telefonico)

- Una versione telefonica del phishing, in cui l'attaccante chiama la vittima fingendo di essere una persona fidata (ad esempio, l'assistenza clienti della banca) per ottenere informazioni.

f. Quid Pro Quo

- L'attaccante offre qualcosa in cambio, ad esempio assistenza tecnica, per convincere la vittima a fornire informazioni o accesso.

g. Dumpster Diving

- Consiste nel cercare informazioni sensibili tra i rifiuti, come documenti aziendali o appunti con password.

h. Impersonation

- L'attaccante finge di essere qualcun altro (ad esempio, un collega o un fornitore) per ottenere informazioni o accesso non autorizzato.

3. Strategie di Difesa contro il Social Engineering

1. Formazione e sensibilizzazione

- È fondamentale educare i dipendenti o gli utenti sulle tecniche di attacco più comuni.
- **Simulazioni periodiche** di attacchi (ad esempio, phishing) possono aiutare a migliorare la consapevolezza.

2. Verifica dell'identità

- Non bisogna mai dare informazioni riservate senza verificare l'identità della persona che le chiede.
- Ad esempio, richiedere un doppio controllo prima di procedere, come una chiamata di conferma.

3. Multi-Factor Authentication (MFA)

- Aggiungere un ulteriore livello di sicurezza, come un codice inviato al telefono, oltre alla password.
- Anche se un attaccante riesce a ottenere la password, non potrà accedere senza il secondo fattore.

4. Politica del Minimo Accesso Necessario

- Dare ai dipendenti solo gli accessi strettamente necessari per il loro lavoro.
- Ridurre gli accessi diminuisce il danno in caso di compromissione di un account.

5. Protezione contro il phishing

- Utilizzare filtri e-mail avanzati per rilevare e bloccare le e-mail sospette.
- Istruire gli utenti a non cliccare su link sconosciuti o aprire allegati non verificati.

6. Sicurezza fisica

- Implementare sistemi di accesso con badge o codici e addestrare i dipendenti a non far entrare persone non autorizzate.
- **Distruzione sicura dei documenti**: Tutti i documenti contenenti dati sensibili devono essere distrutti (ad esempio, usando trituratori).

7. Password forti e gestori di password

- Le password devono essere complesse, lunghe e uniche per ogni account.
- **Gestori di password** possono aiutare a creare e memorizzare password sicure senza che l'utente debba ricordarle tutte.

8. Segnalazione di attività sospette

- Creare un ambiente in cui le persone siano incoraggiate a segnalare attività o e-mail sospette.
- Avere un canale sicuro e facile per la segnalazione.

9. Limitare le informazioni personali online

- Gli attaccanti raccolgono spesso informazioni dalle fonti pubbliche per personalizzare i loro attacchi.
- Evitare di pubblicare troppi dettagli personali sui social media.

10. Piani di risposta agli incidenti

- Avere un piano ben definito per rispondere a violazioni o attacchi.
- Assicurarsi che tutti sappiano come reagire in caso di compromissione.

Conclusione

Il social engineering sfrutta la vulnerabilità umana, ma con una combinazione di **formazione, consapevolezza e misure tecniche**, è possibile ridurre significativamente i rischi. Creare una forte **cultura della sicurezza** all'interno di un'organizzazione o in ambito personale è fondamentale per proteggersi da queste minacce.

Esempi di Tecniche di Social Engineering

1. Phishing – Esempio concreto:

Un dipendente riceve un'e-mail che sembra provenire dal reparto IT della sua azienda. L'e-mail dice che è necessario cambiare la password di accesso al sistema aziendale e include un link. Cliccando su questo link, il dipendente viene reindirizzato a una pagina simile a quella ufficiale dell'azienda, dove inserisce la sua attuale password e la nuova. Tuttavia, è una pagina falsa, e l'attaccante ottiene così la password.

Strategia di difesa: Il dipendente dovrebbe essere istruito a **non cliccare sui link delle e-mail sospette** e a contattare direttamente il reparto IT per conferma. Inoltre, la compagnia dovrebbe usare l’autenticazione multi-fattore, che impedirebbe l’accesso anche in caso di furto della password.

2. Tailgating – Esempio concreto:

Un attaccante aspetta fuori da un edificio aziendale fino a quando un dipendente si avvicina all'ingresso. Con una scusa, come "ho dimenticato il badge", chiede gentilmente di entrare insieme. Il dipendente, per cortesia, gli tiene aperta la porta, permettendo all'attaccante di accedere a un'area riservata senza autorizzazione.

Strategia di difesa: I dipendenti devono essere formati a non far entrare persone senza badge o senza autorizzazione. Ogni persona deve accedere da sola con il proprio badge.

3. Pretexting – Esempio concreto:

Un attaccante chiama un dipendente di una banca fingendo di essere un investigatore della polizia, chiedendo l'accesso ai registri dei clienti per un'indagine. Con un tono autoritario, convince il dipendente a fornire informazioni riservate sui clienti, come numeri di conto e saldi.

Strategia di difesa: Il dipendente deve sempre verificare l'identità della persona che richiede informazioni sensibili, magari tramite una procedura aziendale che richiede l'approvazione del superiore o un contatto ufficiale verificato.

4. Baiting – Esempio concreto:

Un attaccante lascia una chiavetta USB nel parcheggio di un'azienda con l'etichetta "Buste paga". Un dipendente curioso la raccoglie e la inserisce nel suo computer per vedere di cosa si tratta. La chiavetta contiene malware che infetta il sistema della compagnia, fornendo all'attaccante accesso ai dati aziendali.

Strategia di difesa: I dipendenti dovrebbero essere formati a **non inserire mai dispositivi esterni** sconosciuti nei computer aziendali. Le aziende possono implementare politiche che bloccano l'uso di dispositivi USB non autorizzati.

5. Vishing (Phishing telefonico) – Esempio concreto:

Un attaccante chiama una vittima fingendo di essere un rappresentante del servizio clienti di una banca. Dice che ci sono stati tentativi sospetti di accesso all'account della vittima e che è necessario confermare i dati personali, come il numero della carta di credito e il codice di sicurezza. La vittima, preoccupata, fornisce le informazioni richieste, che vengono poi utilizzate per truffe finanziarie.

Strategia di difesa: Le banche non chiedono mai informazioni sensibili per telefono. In caso di chiamate sospette, la vittima dovrebbe interrompere la conversazione e chiamare la banca utilizzando un numero ufficiale, verificato.

6. Quid Pro Quo – Esempio concreto:

Un attaccante si presenta come un tecnico informatico che offre assistenza gratuita per risolvere problemi di rete o software. In cambio, chiede alla vittima di disattivare temporaneamente il software antivirus o di fornire le credenziali di accesso. Una volta ottenuto l'accesso, può infettare il sistema o rubare dati sensibili.

Strategia di difesa: È importante **non accettare assistenza tecnica da fonti non autorizzate**. Qualsiasi intervento esterno dovrebbe passare da procedure aziendali ufficiali e verificate.

7. Dumpster Diving – Esempio concreto:

Un attaccante cerca documenti sensibili nei rifiuti aziendali, come fogli di carta con password scritte o stampe di report finanziari. Queste informazioni vengono poi usate per pianificare un attacco informatico o truffe finanziarie.

Strategia di difesa: Le aziende devono implementare una politica di **distruzione sicura dei documenti** attraverso trituratori o servizi di smaltimento specializzati.

Esempi di Difesa Implementata:

1. Simulazioni di Phishing in Azienda

Un'azienda realizza regolarmente **simulazioni di phishing** per valutare la preparazione dei dipendenti. In queste simulazioni, vengono inviate e-mail false simili a quelle di un attacco phishing reale. I dipendenti che cadono nella trappola ricevono una formazione aggiuntiva per migliorare la loro consapevolezza.

Obiettivo: Aumentare la capacità di riconoscere tentativi di phishing reali.

2. Uso di Badge Elettronici

In una grande azienda tecnologica, l'accesso a qualsiasi edificio è controllato da badge elettronici personali, e il sistema registra chi entra e chi esce. Nessuno può entrare senza il proprio badge, e chi viene scoperto a fare tailgating riceve un avviso disciplinare.

Obiettivo: Garantire che solo personale autorizzato acceda agli spazi aziendali.

3. Implementazione del MFA

Un ente governativo introduce l'autenticazione multi-fattore (MFA) per tutti i dipendenti. Anche se qualcuno riesce a rubare le credenziali di un dipendente, non può accedere ai sistemi aziendali senza il secondo fattore, ad esempio un codice inviato al cellulare.

Obiettivo: Rendere più difficile per gli attaccanti accedere ai sistemi solo con la password.

Conclusione

Gli esempi pratici dimostrano come il social engineering possa colpire in contesti quotidiani e attraverso tecniche semplici ma efficaci. Difendersi da questi attacchi richiede una combinazione di **educazione, tecnologia e procedure ben definite**. Una cultura della sicurezza informatica, che coinvolga tutti i membri di un'organizzazione, è il miglior scudo contro queste minacce.

Ecco un elenco di alcune vulnerabilità note (CVE) relative a Windows 10, insieme a dettagli e soluzioni consigliate per proteggersi dagli attacchi:

1. CVE-2024-43491 - Windows Update Use-After-Free Vulnerability

- **Descrizione**: Si tratta di una vulnerabilità "use-after-free" nel servizio Windows Update che può essere sfruttata per eseguire codice arbitrario da remoto. Questo tipo di attacco consente a un hacker di ottenere il controllo completo del sistema bersaglio senza necessità di interazione dell'utente.
- **Gravità**: Critico (punteggio CVSS 9.8/10).
- **Impatto**: Se sfruttato, l'attaccante può causare il crash del sistema o eseguire codice malevolo con privilegi elevati, mettendo a rischio la sicurezza dell'intero sistema.

- **Soluzione**: Installare immediatamente le patch di sicurezza fornite da Microsoft (CISA) (NVD).

2. CVE-2020-0601 - CryptoAPI Spoofing Vulnerability

- **Descrizione**: Questa vulnerabilità nel componente Windows CryptoAPI (Crypt32.dll) riguarda la gestione delle firme digitali ECC. Permette a un attaccante di far sembrare legittimo un certificato falsificato, potenzialmente ingannando gli utenti a installare software malevolo firmato digitalmente.
- **Impatto**: Un exploit di questa vulnerabilità può portare a un attacco man-in-the-middle o alla decrittazione di informazioni riservate, come dettagli finanziari.
- **Soluzione**: Applicare le patch rilasciate da Microsoft per correggere la gestione delle firme digitali nel sistema (CISA) (Microsoft Security Response Center).

3. CVE-2020-0609/CVE-2020-0610 - Remote Desktop Gateway Vulnerabilities

- **Descrizione**: Queste vulnerabilità permettono l'esecuzione remota di codice sui server Windows attraverso l'uso del protocollo Remote Desktop (RDP). L'attacco non richiede autenticazione e può avvenire senza interazione dell'utente.
- **Impatto**: Un attaccante potrebbe eseguire codice arbitrario sul server compromesso, ottenendo il pieno controllo del sistema.
- **Soluzione**: Installare immediatamente le patch disponibili e limitare l'accesso RDP ai soli utenti e reti autorizzate (CISA) (Microsoft Security Response Center).

4. CVE-2024-38014 - Windows Installer Privilege Escalation

- **Descrizione**: Una vulnerabilità nel servizio Windows Installer che permette a un attaccante di ottenere privilegi di livello SYSTEM. L'attacco può essere eseguito tramite manipolazioni nell'installazione di applicazioni mal configurate.
- **Impatto**: Può consentire a un attaccante di prendere il controllo completo del sistema.
- **Soluzione**: Applicare le patch più recenti e rivedere le configurazioni di sicurezza per il servizio Windows Installer (Cisco Talos Blog).

Misure di Difesa Generali:

1. **Patch regolari**: Mantenere Windows e tutte le applicazioni aggiornate applicando tempestivamente le patch di sicurezza.
2. **Gestione delle autorizzazioni**: Limitare i privilegi degli utenti e proteggere i servizi esposti, come RDP, con meccanismi di autenticazione forti.
3. **Strumenti di monitoraggio**: Implementare strumenti di rilevamento delle intrusioni per monitorare eventuali attività sospette.

4. **Firewall e VPN**: Usare firewall per limitare l'accesso ai servizi critici e VPN per l'accesso remoto sicuro.

Integrare queste misure nella tua strategia di sicurezza aziendale ridurrà significativamente il rischio di sfruttamento di queste vulnerabilità.