Report: Social Engineering e le sue Tecniche più Comuni

1. Cos'è il Social Engineering?

Il **Social Engineering** è una forma di attacco psicologico e manipolazione che mira a sfruttare le debolezze umane per ottenere accesso non autorizzato a informazioni sensibili, sistemi informatici o risorse aziendali. Gli attaccanti utilizzano tecniche psicologiche per convincere le vittime a rivelare dati riservati, come password, informazioni personali, dettagli bancari, o persino a fornire accesso fisico ai locali aziendali. Piuttosto che concentrarsi solo sulle vulnerabilità tecniche, il social engineering sfrutta l'elemento umano, spesso considerato l'anello più debole nella sicurezza informatica.

2. Obiettivi del Social Engineering

Gli attacchi di social engineering mirano generalmente a:

- **Ottenere informazioni sensibili** (come password o dati personali).
- **Compromettere account** (personali o aziendali).
- **Accedere a risorse aziendali** (fisiche o digitali).
- **Diffondere malware** o altre minacce informatiche.

Gli attacchi di social engineering possono avere impatti devastanti, sia in termini di perdite finanziarie che di danni alla reputazione. Gli aggressori spesso fanno affidamento su una combinazione di empatia, urgenza e autorevolezza per manipolare le loro vittime.

---

3. Tecniche Comuni di Social Engineering

3.1 Phishing

Il **phishing** è una delle tecniche di social engineering più conosciute e diffuse, progettata per ingannare le vittime inducendole a rivelare informazioni personali o finanziarie. Gli attaccanti usano comunicazioni apparentemente legittime, spesso tramite email, SMS o messaggi sui social, per convincere le persone a cliccare su link dannosi o a scaricare allegati malevoli.

Tipi di Phishing:

- **Email Phishing**: L'attaccante invia email che sembrano provenire da aziende legittime (ad esempio banche, servizi di pagamento online) e richiede alla vittima di fornire informazioni sensibili.
- **Spear Phishing**: Questo attacco è mirato e personalizzato; l'attaccante raccoglie informazioni specifiche sulla vittima per rendere il messaggio più credibile.
- **Whaling**: È simile allo spear phishing ma prende di mira figure di alto livello, come dirigenti o manager, sfruttando la loro posizione di autorità.

- **Vishing** (voice phishing): Gli attaccanti chiamano le vittime fingendosi operatori di supporto clienti e richiedono informazioni personali o credenziali di accesso.

3.2 Tailgating

Il **tailgating** è una tecnica di social engineering fisica che consiste nell'entrare in aree riservate "attaccandosi" a una persona autorizzata. Gli attaccanti possono, ad esempio, aspettare che una porta si apra, per poi seguirne rapidamente una persona fidata o addirittura chiedere di tener loro la porta aperta, facendo finta di aver dimenticato il badge o altre credenziali.

Esempi comuni di tailgating:

- **Approccio amichevole**: L'attaccante si presenta come un collega o un fornitore e cerca di entrare in azienda "di soppiatto", sfruttando la cortesia del personale.
- **Uso di oggetti di scena**: Per aumentare la credibilità, possono utilizzare oggetti come tesserini contraffatti, divise o attrezzature professionali.
- **Entrata di massa**: Durante eventi o pause di gruppo, come pranzo o cambio turno, i tailgater possono confondersi tra il personale che rientra insieme, rendendo più difficile individuare l'intruso.

3.3 Pretexting

Il **pretexting** si basa sulla costruzione di uno scenario o "pretesto" convincente per indurre una vittima a fornire informazioni personali o aziendali. L'attaccante finge di essere una figura di autorità (es. un agente di polizia, un rappresentante di una banca o un tecnico IT) per stabilire fiducia e legittimità.

Esempi di pretexting:

- Un attaccante si spaccia per un dipendente del reparto IT e chiede informazioni di accesso per "verificare" il sistema.
- Un individuo si presenta come un fornitore e richiede dati specifici sulle procedure interne per "aggiornare i file" o gestire una "richiesta urgente".

3.4 Baiting

Il **baiting** è una tecnica che fa leva sulla curiosità delle persone, offrendo una sorta di "esca" per convincere le vittime a scaricare malware o a fornire informazioni. Un esempio comune di baiting è l'uso di chiavette USB infette lasciate in aree accessibili, come il parcheggio di un'azienda, sperando che qualcuno le raccolga e le inserisca in un computer aziendale.

3.5 Quid Pro Quo

Il **quid pro quo** è una tecnica di scambio in cui l'attaccante promette un beneficio (come assistenza tecnica o un premio) in cambio di informazioni sensibili o dell'esecuzione di determinate azioni da parte della vittima. È spesso utilizzato per ottenere credenziali di accesso o per convincere la vittima a disabilitare misure di sicurezza.

---

4. Strategie per Prevenire il Social Engineering

La prevenzione del social engineering si basa su tre pilastri principali:

- **Educazione e Formazione**: È fondamentale addestrare il personale a riconoscere i segnali di attacco e sensibilizzarlo sui rischi delle tecniche di social engineering.
- **Implementazione di Procedure di Sicurezza**: Procedure come l'utilizzo di badge identificativi, l'autenticazione a più fattori (MFA) e la verifica dell'identità delle persone prima di condividere informazioni possono ridurre i rischi.
- **Simulazioni di Attacco**: Le simulazioni, come le esercitazioni di phishing, aiutano il personale a identificare potenziali attacchi e ad agire in modo appropriato senza cadere nella trappola degli attaccanti.

---

5. Conclusione

Il social engineering rappresenta una minaccia significativa per individui e organizzazioni, sfruttando l'elemento umano come mezzo per violare i sistemi di sicurezza. Con l'evolversi delle tecnologie e delle comunicazioni, le tecniche di social engineering continuano a rafforzarsi e diventano sempre più sofisticate. La migliore difesa contro queste minacce è la consapevolezza e la preparazione, facendo in modo che ogni individuo possa riconoscere, resistere e rispondere a queste forme di manipolazione.

Strategie per Difendersi dagli Attacchi di Social Engineering

1. **Formazione e Sensibilizzazione del Personale**
    - **Come funziona**: La formazione regolare su come riconoscere gli attacchi di social engineering è fondamentale. Questo include insegnare al personale a identificare segnali sospetti in email, telefonate e interazioni personali. Gli utenti devono essere informati sulle varie tecniche, come phishing e pretexting, e sapere come agire di fronte a una potenziale minaccia.
    - **Perché è importante**: La maggior parte degli attacchi di social engineering mira a sfruttare la scarsa consapevolezza. I dipendenti formati sono in grado di riconoscere tentativi di attacco prima che possano compromettere la sicurezza aziendale.
2. **Autenticazione a Due Fattori (2FA)**
    - **Come funziona**: La 2FA richiede agli utenti di confermare la propria identità tramite due forme di verifica, come una password e un codice temporaneo inviato al telefono o una scansione biometrica. Anche se un attaccante riesce a ottenere una password, non può accedere ai sistemi senza il secondo fattore.
    - **Perché è importante**: L'autenticazione a due fattori aggiunge un ulteriore livello di sicurezza che rende più difficile per gli attaccanti ottenere accesso a sistemi e informazioni sensibili.
3. **Politiche di Accesso e Badge di Identificazione**
    - **Come funziona**: Implementare politiche rigorose per l'accesso fisico ai locali, usando badge identificativi e altre misure di autenticazione. Gli ingressi dovrebbero essere monitorati, e solo il personale autorizzato deve avere accesso a determinate aree.
    - **Perché è importante**: Le misure fisiche come i badge impediscono l'accesso non autorizzato e riducono il rischio di attacchi come il tailgating. Questi controlli assicurano che solo chi ha un reale permesso possa entrare in aree riservate.
4. **Simulazioni di Phishing e Test di Social Engineering**
    - **Come funziona**: Simulazioni periodiche di phishing e altri test aiutano a misurare quanto i dipendenti siano preparati a identificare gli attacchi di social engineering. Questi test consistono in tentativi controllati di phishing o richieste di informazioni che servono a valutare la reazione del personale.
    - **Perché è importante**: Le simulazioni aiutano a migliorare la consapevolezza e a identificare aree di debolezza nella formazione del personale. Inoltre, consentono di aggiornare le strategie di difesa in base ai risultati ottenuti.
5. **Verifica dell'Identità nelle Comunicazioni Sensibili**
    - **Come funziona**: Se viene richiesta una condivisione di informazioni sensibili, è importante verificare sempre l'identità del richiedente. Questo può essere fatto richiamando direttamente l'organizzazione o la persona richiedente attraverso i contatti ufficiali e non tramite i numeri forniti durante la richiesta stessa.
    - **Perché è importante**: La verifica dell'identità riduce il rischio di cadere vittima del pretexting e di altre tecniche in cui l'attaccante si finge un'autorità o una figura fidata.
6. **Limitare l'Accesso alle Informazioni Sensibili**

    - **Come funziona**: Assegnare a ciascun dipendente solo le informazioni e i privilegi necessari per svolgere il proprio ruolo (principio del "least privilege"). Inoltre, l'accesso dovrebbe essere tracciato e monitorato per individuare attività insolite.
    - **Perché è importante**: Limitare l'accesso riduce la quantità di informazioni che un attaccante potrebbe ottenere nel caso in cui riesca a violare la sicurezza di un individuo o un account.
7. **Controllo delle Fonti di Informazioni e Dati**
    - **Come funziona**: Verifica dell'autenticità delle fonti da cui provengono informazioni o link, soprattutto nelle comunicazioni email o sui social media. Le persone dovrebbero essere incoraggiate a non cliccare su link o scaricare allegati provenienti da fonti non verificate.
    - **Perché è importante**: Il controllo delle fonti aiuta a prevenire attacchi di phishing e baiting, dove link o allegati dannosi vengono usati per installare malware o rubare dati.

Conclusione Finale

Un'efficace strategia di difesa contro il social engineering richiede un mix di consapevolezza, formazione e tecnologia. Con le giuste misure preventive e un'attenta vigilanza, aziende e individui possono proteggersi dai tentativi di manipolazione degli attaccanti e garantire la sicurezza delle proprie risorse e informazioni.

Windows 10 CVE

Windows 10 presenta diverse vulnerabilità catalogate come CVE (Common Vulnerabilities and Exposures), che riguardano componenti critici del sistema. Ecco alcuni esempi recenti:

1. **CVE-2022-34722**: Una vulnerabilità di esecuzione di codice da remoto nel protocollo IKE, con un punteggio di gravità di 9.8. Consente agli aggressori di eseguire codice arbitrario e compromette la sicurezza della rete.
2. **CVE-2022-35793**: Problema nell'elevazione dei privilegi del servizio Windows Print Spooler, utilizzabile per ottenere privilegi amministrativi.
3. **CVE-2022-35831**: Riguarda un'informazione non autorizzata nel Remote Access Connection Manager, che potrebbe rivelare informazioni sensibili.

Per prevenire tali vulnerabilità, Microsoft raccomanda l'aggiornamento costante dei sistemi e l'adozione di configurazioni di sicurezza avanzate. Per un elenco completo e soluzioni specifiche, è possibile consultare siti come OpenCVE o il Microsoft Security Response Center.

Fonti:
https://app.opencve.io/cve/?vendor=microsoft&product=windows_10