

S5/L4

Potresti spiegare cos'è il social engineering e descrivere le tecniche più comuni utilizzate dagli attaccanti, come phishing e tailgating?

Il social engineering (ingegneria sociale) è una tecnica di attacco informatico che sfrutta la manipolazione psicologica delle persone per ottenere informazioni riservate, accesso a sistemi protetti o eseguire azioni dannose. Invece di cercare vulnerabilità tecniche nei sistemi, gli attaccanti puntano sulle debolezze umane, inducendo le vittime a rivelare password, dati sensibili o a compiere azioni che compromettono la sicurezza.

Tecniche più comuni di social engineering

1. Phishing


Il phishing è una tecnica in cui gli attaccanti inviano e-mail, messaggi o creano siti web falsi per indurre le vittime a fornire informazioni sensibili come credenziali, numeri di carte di credito o dati aziendali.

Varianti del phishing:

- **Spear Phishing:** Attacco mirato a un individuo o un'organizzazione specifica, con messaggi personalizzati.
- **Whaling:** Phishing mirato a dirigenti o persone di alto profilo in un'azienda.
- **Smishing:** Phishing via SMS.
- **Vishing:** Phishing via chiamate vocali, spesso con l'uso di falsi operatori bancari o di supporto tecnico.


2. Tailgating (o Piggybacking)

Il tailgating consiste nel seguire una persona autorizzata per entrare in un'area riservata senza permessi.

 **Esempio:** Un attaccante si avvicina a un dipendente che entra in un edificio aziendale e, fingendo di aver dimenticato il badge, lo convince a tenere la porta aperta.


3. Pretexting

Si tratta di creare un pretesto credibile per convincere la vittima a fornire informazioni riservate.

 **Esempio:** Un attaccante si spaccia per un dipendente del reparto IT e chiede a un collega di comunicargli la password per risolvere un problema tecnico.


4. Baiting

Il baiting (esca) attira le vittime con qualcosa di allettante per indurle a eseguire azioni pericolose.

 **Esempio:** Un attaccante lascia una chiavetta USB infetta in un parcheggio aziendale con un'etichetta come "Stipendi 2025". Se un dipendente la inserisce nel PC, può compromettere il sistema.

5. Quid Pro Quo

Si basa sulla promessa di un vantaggio in cambio di informazioni o azioni non sicure.

 **Esempio:** Un finto tecnico IT chiama un dipendente, offrendosi di migliorare le prestazioni del suo computer in cambio della password di accesso.

6. Shoulder Surfing

Tecnica in cui l'attaccante osserva direttamente una persona mentre inserisce credenziali o dati sensibili.

💡 **Esempio:** Guardare sopra la spalla di un dipendente mentre digita la password su un computer o un bancomat.

🔒 Come difendersi dal social engineering?

- ✓ **Verifica sempre l'identità** di chi richiede informazioni riservate.
- ✓ **Non cliccare su link sospetti** e controlla sempre gli URL nei messaggi.
- ✓ **Non condividere informazioni sensibili** via e-mail o telefono senza confermare l'autenticità del richiedente.
- ✓ **Blocca l'accesso fisico** ai luoghi riservati e non lasciare porte aperte a sconosciuti.
- ✓ **Fai attenzione a chi ti osserva** mentre inserisci password o dati riservati.
- ✓ **Usa l'autenticazione a due fattori (2FA)** per proteggere gli account.
- ✓ **Sottoporti il personale a formazione** sulla sicurezza per riconoscere e prevenire attacchi.

Potresti elencare e spiegare alcune strategie efficaci per difendersi dagli attacchi di social engineering?

Per difendersi efficacemente dagli attacchi di social engineering, è fondamentale adottare un approccio multilivello che combini consapevolezza, tecnologia e procedure aziendali. Ecco alcune strategie efficaci:

1. Formazione e sensibilizzazione 🎓

💡 **Perché è importante?** Il social engineering si basa sull'errore umano. Dipendenti e utenti informati sono la prima linea di difesa.

✅ **Azioni concrete:**

- Organizzare **corsi di formazione periodici** su sicurezza informatica e social engineering.
- Simulare attacchi di phishing per testare la prontezza del personale.
- Insegnare a **riconoscere segnali sospetti** (es. email con toni urgenti, richieste insolite di dati).

2. Verifica dell'identità ID

💡 **Perché è importante?** Gli attaccanti spesso si spacciano per persone di fiducia.

✅ **Azioni concrete:**

- **Non fornire mai informazioni riservate** senza una verifica diretta dell'identità.
- Usare una **doppia verifica** (es. chiamare direttamente il collega per confermare una richiesta).
- Implementare **badge e controlli biometrici** per limitare l'accesso fisico alle aree sensibili.


3. Protezione contro il phishing ✉️

💡 **Perché è importante?** Il phishing è una delle tecniche di attacco più diffuse.

✅ **Azioni concrete:**

- **Non cliccare su link sospetti** o aprire allegati non richiesti.
- Passare il **cursore sopra i link** per verificare l'URL prima di cliccare.
- Attivare **filtri anti-phishing** nei client di posta elettronica.


4. Utilizzo dell'autenticazione a più fattori (MFA)

 **Perché è importante?** Anche se un attaccante ruba una password, senza il secondo fattore di autenticazione non potrà accedere.

Azioni concrete:

- **Attivare l'MFA su tutti gli account sensibili** (email aziendale, VPN, account cloud).
- Preferire autenticazioni con **app di verifica** (es. Google Authenticator) anziché SMS, che possono essere intercettati.


5. Limitare il principio dei privilegi minimi

 **Perché è importante?** Se un attaccante compromette un account, meno privilegi ha l'utente, meno danni può fare.

Azioni concrete:

- Concedere **accesso solo alle informazioni e ai sistemi strettamente necessari**.
- Implementare **controlli sugli account privilegiati** e monitorare le loro attività.
- Utilizzare **account separati per utenti standard e amministratori IT**.


6. Sicurezza fisica e contro il tailgating

 **Perché è importante?** Gli attaccanti possono ottenere accesso fisico ai sistemi con metodi come il tailgating.

Azioni concrete:

- **Non tenere aperte le porte a sconosciuti**, anche se sembrano persone fidate.
- Installare **lettori di badge, telecamere di sorveglianza e controlli biometrici**.
- Implementare la politica del "**challenge culture**", dove i dipendenti possono chiedere l'identità di chi cerca di entrare in aree riservate.

7. Protezione contro il baiting (ingegneria sociale tramite oggetti fisici)

 **Perché è importante?** Un attaccante può lasciare una chiavetta USB infetta in un luogo visibile sperando che qualcuno la inserisca nel PC.

Azioni concrete:

- **Non inserire mai dispositivi sconosciuti** nei computer aziendali.
- Disabilitare l'**auto-esecuzione delle unità USB** sui computer aziendali.
- Implementare **soluzioni di sicurezza endpoint** per rilevare malware da dispositivi esterni.

8. Creazione di una cultura della sicurezza

 **Perché è importante?** Una sicurezza efficace si basa su una mentalità aziendale condivisa.

Azioni concrete:

- Creare **politiche di sicurezza aziendale chiare** e facili da seguire.
- Premiare e riconoscere i dipendenti che segnalano tentativi di social engineering.
- Rendere la sicurezza una **responsabilità condivisa** e non solo un compito dell'IT.

9. Monitoraggio e risposta agli incidenti 🧑

💡 **Perché è importante?** Anche con tutte le precauzioni, gli attacchi possono avvenire.

✅ **Azioni concrete:**

- Implementare un **SOC (Security Operations Center)** per monitorare attività sospette.
- Usare **sistemi SIEM (Security Information and Event Management)** per analizzare i log e rilevare anomalie.
- Creare un **piano di risposta agli incidenti** con procedure precise su come reagire in caso di attacco.

10. Segnalazione e test di sicurezza regolari 🛡️

💡 **Perché è importante?** La sicurezza deve essere continuamente aggiornata e testata.

✅ **Azioni concrete:**

- Effettuare **penetration test e red teaming** per simulare attacchi di social engineering.
- Analizzare i **log di accesso e le attività sospette** in modo proattivo.
- Avere un **canale di segnalazione anonimo** per i dipendenti che sospettano attività di social engineering.

Conclusione

Nessuna singola misura è sufficiente per fermare il social engineering, ma una combinazione di **consapevolezza, tecnologia e processi di sicurezza ben definiti** può ridurre significativamente i rischi.

Potresti fornirmi una lista dei CVE relativi a Windows 10? Vorrei anche informazioni dettagliate su alcuni di essi, inclusi i dettagli delle vulnerabilità e le soluzioni consigliate.

Windows 10 ha registrato diverse vulnerabilità nel corso degli anni, identificate attraverso il sistema **Common Vulnerabilities and Exposures (CVE)**. Ecco una panoramica di alcune di queste vulnerabilità, con dettagli specifici e soluzioni consigliate:

1. CVE-2024-43491

Descrizione: Questa vulnerabilità riguarda lo **Stack di Servizio** di Windows 10 versione 1507. Un problema nello stack ha causato il rollback delle correzioni per alcune vulnerabilità che interessano i componenti opzionali, rendendo nuovamente esposte le falle precedentemente mitigate.

Impatto: Un attaccante potrebbe sfruttare queste vulnerabilità ripristinate per compromettere il sistema.

Soluzione: Microsoft ha rilasciato aggiornamenti per risolvere questo problema. È fondamentale assicurarsi che tutti gli aggiornamenti di sicurezza più recenti siano installati.

2. CVE-2018-3665 (Lazy FP State Restore)

Descrizione: Questa vulnerabilità riguarda l'esecuzione speculativa del canale laterale, nota come "Lazy FP State Restore".

Impatto: Un attaccante potrebbe sfruttare questa vulnerabilità per accedere a informazioni sensibili attraverso l'esecuzione speculativa.

Soluzione: Microsoft ha fornito linee guida e aggiornamenti per mitigare questa vulnerabilità. È consigliabile consultare l'avviso di sicurezza ADV180016 e applicare le patch appropriate.

3. CVE-2018-0775

****Descrizione:**** Una vulnerabilità in Microsoft Edge su Windows 10 versione 1709 permette a un attaccante di eseguire codice arbitrario nel contesto dell'utente corrente, a causa di come il motore di scripting gestisce gli oggetti in memoria.

Impatto: Un attaccante potrebbe ottenere gli stessi privilegi dell'utente corrente, potendo installare programmi, visualizzare, modificare o eliminare dati, o creare nuovi account con diritti completi.

Soluzione: Microsoft ha rilasciato aggiornamenti di sicurezza per affrontare questa vulnerabilità. È essenziale mantenere il sistema aggiornato con le ultime patch disponibili.

Raccomandazioni Generali

- **Aggiornamenti Regolari:** Assicurarsi di installare tempestivamente tutti gli aggiornamenti di sicurezza rilasciati da Microsoft per proteggere il sistema dalle vulnerabilità note.

- **Monitoraggio delle Vulnerabilità:** Consultare regolarmente fonti affidabili, come il [National Vulnerability Database (NVD)](<https://nvd.nist.gov/>) e il [sito ufficiale di Microsoft](<https://msrc.microsoft.com/>), per rimanere informati sulle nuove vulnerabilità e sulle relative soluzioni.

- **Implementazione di Misure di Sicurezza:** Oltre agli aggiornamenti, adottare misure di sicurezza aggiuntive come l'uso di software antivirus aggiornati, firewall e pratiche di navigazione sicura.

Per una lista completa e dettagliata delle vulnerabilità associate a Windows 10, è possibile consultare il sito CVE Details (https://www.cvedetails.com/product/32238/Microsoft-Windows-10.html?vendor_id=26).