SOCIAL ENGINEERING E TECNICHE DI DIFESA

Il **social engineering** è una tecnica di manipolazione psicologica utilizzata per indurre le persone a divulgare informazioni sensibili, concedere accesso a sistemi o compiere azioni specifiche. Gli attaccanti sfruttano la fiducia, l'urgenza o la curiosità delle vittime per ottenere ciò che desiderano, senza dover utilizzare metodi tecnici complessi.

Tecniche più comuni di social engineering

1. ## PHISHING
   Il phishing è una forma molto diffusa di social engineering. Consiste nell'inviare messaggi (solitamente e-mail, SMS o messaggi sui social media) che sembrano provenire da una fonte affidabile, come una banca, un'azienda o un collega.
   Obiettivo: Ingannare la vittima per farle:
   - Cliccare su un link che porta a un sito falso.
   - Inserire credenziali, informazioni personali o finanziarie.
   - Scaricare malware.

     Esempio: Un'email che sembra provenire dalla tua banca ti chiede di "verificare il tuo account" cliccando su un link.
2. ## SPEAR PHISHING
   Variante del phishing, ma altamente mirata. L'attaccante personalizza i messaggi utilizzando informazioni specifiche sulla vittima (ad esempio, conoscendo il suo ruolo lavorativo o i suoi interessi).
   Esempio: Un dirigente riceve un'email che sembra provenire dal CEO dell'azienda, chiedendo un trasferimento urgente di fondi.
3. ## TAILGATING (o Piggybacking)
   Con questa tecnica, un attaccante si infiltra fisicamente in un'area protetta seguendo da vicino una persona autorizzata che accede.
   Obiettivo: Ottenere accesso a uffici, server room o aree riservate.
   Esempio: Un attaccante si avvicina a un dipendente all'entrata, fingendo di aver dimenticato il badge, e si fa tenere la porta aperta.
4. ## PRETEXTING
   Gli attaccanti inventano un pretesto o una storia convincente per ottenere informazioni o favori dalla vittima.
   Obiettivo: Creare una falsa identità o scenario credibile per manipolare la vittima.
   Esempio: Qualcuno chiama un dipendente fingendo di essere dell'assistenza IT e chiede le credenziali per risolvere un "problema urgente".
5. ## BAITING
   Gli attaccanti offrono un incentivo (esca) per indurre la vittima a compiere un'azione. Può essere un oggetto fisico (come una chiavetta USB infetta) o un'offerta online.
   Esempio: Una chiavetta USB con l'etichetta "Riservato" viene lasciata in un'area pubblica. Una persona curiosa la inserisce nel computer, attivando malware.
6. ## VISHING (Voice Phishing)
   Variante del phishing che utilizza telefonate o messaggi vocali per ottenere informazioni.
   Esempio: Una persona finge di essere un rappresentante di un istituto finanziario e convince la vittima a rivelare il PIN del conto.
7. ## QUID PRO QUO
   Qui si promette qualcosa in cambio di informazioni o accesso.

Esempio: Un attaccante chiama un dipendente dicendo di offrire assistenza tecnica gratuita in cambio delle credenziali.

8. **SHOULDER SURFING**
   Gli attaccanti osservano fisicamente o con strumenti la vittima mentre digita password o PIN.
   Esempio: Guardare sopra la spalla di qualcuno mentre inserisce il codice al bancomat.

Difendersi dagli attacchi di **social engineering** richiede un approccio combinato di consapevolezza, strumenti tecnologici e buone pratiche. Ecco alcune strategie efficaci:

---

1. Educazione e consapevolezza

- **Formazione regolare**: Organizza corsi di formazione per i dipendenti e sensibilizza sulla sicurezza informatica.
- **Simulazioni di attacco**: Esegui test di phishing o tailgating per valutare il livello di consapevolezza e migliorare le difese.
- **Conoscenza dei segnali di allarme**: Impara a riconoscere messaggi con urgenze sospette, errori grammaticali o richieste di informazioni personali.

---

2. Autenticazione forte

- **Autenticazione a due fattori (2FA)**: Aggiungi un livello di sicurezza extra per accedere ai sistemi. Anche se un attaccante ottiene le credenziali, non potrà accedere senza il secondo fattore.
- **Password uniche e robuste**: Utilizza password lunghe, complesse e diverse per ogni account.
- **Gestori di password**: Usa strumenti sicuri per generare e memorizzare password complesse.

---

3. Verifica delle comunicazioni

- **Conferma diretta**: Se ricevi una richiesta sospetta via email o telefono, contatta direttamente la persona o l'organizzazione per verificare.
- **Diffida delle richieste urgenti**: Gli attaccanti spesso creano un senso di urgenza. Prenditi sempre il tempo necessario per valutare la situazione.
- **Controlla le fonti**: Verifica attentamente i mittenti delle email (spesso gli indirizzi falsi sono simili ma non identici a quelli legittimi).

---

4. Limitazione delle informazioni

- **Condivisione minima**: Non condividere informazioni personali o aziendali sensibili senza una verifica adeguata.
- **Social media**: Limita le informazioni personali pubbliche sui tuoi profili social, che potrebbero essere sfruttate per attacchi mirati.

---

5. Protezione fisica

- **Badge e accessi**: Implementa politiche rigide per l'accesso fisico agli edifici e ai sistemi. Assicurati che ogni dipendente utilizzi il proprio badge e non consenta tailgating.
- **Consegna di dispositivi sospetti**: Non utilizzare chiavette USB o dispositivi sconosciuti trovati in giro.

---

6. Strumenti tecnologici

- **Filtri anti-phishing**: Configura filtri email per bloccare messaggi sospetti.
- **Software antivirus e firewall**: Mantieni attivi e aggiornati i sistemi di protezione per rilevare minacce.
- **Aggiornamenti regolari**: Mantieni software, sistemi operativi e dispositivi sempre aggiornati per chiudere vulnerabilità.

---

7. Monitoraggio e risposta

- **Sistema di monitoraggio**: Utilizza strumenti che rilevano attività insolite nei sistemi.
- **Incident Response Plan**: Prepara un piano per rispondere rapidamente a potenziali attacchi.
- **Segnalazione degli incidenti**: I dipendenti devono sapere a chi segnalare situazioni sospette.

---

8. Politiche aziendali solide

- **Principio del privilegio minimo**: Concedi agli utenti solo l'accesso strettamente necessario per il loro lavoro.
- **Politiche di sicurezza**: Definisci procedure per la gestione delle credenziali, il trattamento delle informazioni sensibili e l'accesso alle risorse aziendali.

---

9. Diffusione della cultura della sicurezza

- **Promuovi l'importanza della sicurezza**: Rendila una priorità e incoraggia i dipendenti a rimanere vigili.
- **Premia la vigilanza**: Ricompensa chi individua e segnala tentativi di attacco.

---

10. Test e miglioramento continuo

- **Penetration Testing**: Simula attacchi per identificare punti deboli e migliorare le difese.
- **Feedback e aggiornamenti**: Integra lezioni apprese da incidenti precedenti o nuove minacce.

Queste strategie, se applicate con costanza e attenzione, possono ridurre significativamente il rischio di essere vittima di attacchi di social engineering.

CVE (Common Vulnerabilities and Exposures)

Ecco una panoramica di alcune vulnerabilità di sicurezza (CVE) relative a Windows 11, incluse le loro descrizioni e le soluzioni suggerite:

1. CVE-2024-21302

Questa vulnerabilità riguarda un problema di elevazione di privilegi nei sistemi che supportano la Virtualization-Based Security (VBS). Un attaccante con privilegi amministrativi potrebbe sostituire file di sistema con versioni obsolete, reintroducendo vulnerabilità già mitigate, bypassando le funzionalità di sicurezza di VBS e accedendo a dati protetti. Microsoft ha rilasciato aggiornamenti di sicurezza nell'agosto 2024, ma gli amministratori devono implementare politiche di revoca opzionali (KB5042562) per mitigare il problema【10】.

2. CVE-2024-6769

Questa vulnerabilità sfrutta il "DLL Hijacking" causato da un'alterazione delle unità e l'avvelenamento della cache di attivazione. Consente a un attaccante autenticato di elevare i privilegi da un processo a media integrità a uno ad alta integrità senza intervento dell'UAC. Colpisce Windows 10, Windows 11 e diverse versioni di Windows Server. Sono disponibili patch e misure per limitare il rischio【12】.

3. CVE-2023-28293

Un problema di elevazione dei privilegi nel kernel di Windows. Gli attaccanti possono sfruttarlo per ottenere privilegi amministrativi su sistemi vulnerabili. Microsoft ha fornito aggiornamenti di sicurezza per mitigare questo problema. È fondamentale installare le ultime patch disponibili per prevenire possibili abusi【13】.

Raccomandazioni Generali

Per mitigare il rischio di queste vulnerabilità:

- **Aggiornamenti regolari:** Installare tempestivamente gli aggiornamenti di sicurezza ufficiali di Microsoft.
- **Monitoraggio dei sistemi:** Utilizzare strumenti di monitoraggio per individuare attività anomale.
- **Applicazione delle best practice:** Implementare policy di accesso con privilegi minimi e proteggere l'accesso amministrativo con autenticazione a più fattori.