Social engineering: analisi e strategie di difesa

Il **social engineering** è una tecnica di manipolazione psicologica utilizzata per ingannare le persone al fine di ottenere informazioni riservate o compiere azioni dannose, come fornire. Gli attaccanti sfruttano la fiducia, la paura oppure l'urgenza, senza ricorrere a metodi tecnici avanzati.

Ho analizzato due attacchi reali di social engineering:

- Caso 1: Phishing e Vishing nel caso Twitter (2020)

Gli hacker hanno utilizzato **Vishing** per ingannare i dipendenti di Twitter: fingendosi membri del supporto IT, hanno ottenuto credenziali di accesso ai sistemi interni. Hanno usato i permessi acquisiti per **hackerare account VIP** e pubblicare tweet fraudolenti per rubare Bitcoin. L'attacco ha portato **a perdite di oltre 100.000 dollari** e danni alla reputazione di Twitter.

Ciò è potuto avvenire per i seguenti motivi:

- **Mancanza di verifica dell'identità** nei contatti tra dipendenti e IT: I dipendenti **non hanno verificato** se la richiesta fosse legittima e hanno fornito i dati, permettendo l'hack degli account VIP.
- **Accesso privilegiato troppo esteso** a molti dipendenti: poiché troppi dipendenti avevano **permessi di amministrazione**, una volta ingannati alcuni di loro, gli hacker hanno **hackerato account VIP** come Elon Musk e Obama.
- **Mancanza di autenticazione a più fattori (MFA)** su account critici. I fattori di autenticazione possono essere:

  Qualcosa che conosci → Password o PIN

  Qualcosa che possiedi → Codice via SMS, app di autenticazione, smart card

  Qualcosa che sei → Impronta digitale, riconoscimento facciale o retina

- Caso 2: Baiting con chiavette USB infette

Gli attaccanti hanno lasciato chiavette USB con nomi accattivanti come **"stipendi 2024"** o **"progetti segreti"**. Un dipendente ne ha inserita una nel PC, attivando **un malware** che ruba dati aziendali o installa un ransomware. Questo tipo di attacco è stato **usato in test di sicurezza aziendali**, con **percentuali di successo superiori al 50%**.

I punti deboli sfruttati dagli attaccanti sono stati i seguenti:

Curiosità e mancanza di formazione sulla sicurezza. **Mancanza di restrizioni su dispositivi USB** nei sistemi aziendali. **Assenza di politiche chiare** su cosa fare in caso di ritrovamento di dispositivi sospetti.

Raccomandazioni sugli attacchi elencati a scopo di prevenzione

- **Phishing e Vishing**

Implementare **filtri anti-phishing avanzati** sulle email aziendali.
Formare i dipendenti a **riconoscere email e telefonate sospette**.
Mai fornire credenziali via telefono o email, anche se richiesto da "colleghi" o "IT".
Autenticazione a più fattori (MFA) per tutti gli accessi critici.
Creare una **procedura interna per verificare richieste sospette**, es. contattare direttamente il reparto IT.

- **Baiting e uso di USB infette**

Vietare l'uso di chiavette USB sconosciute nei computer aziendali.
Disabilitare **l'auto-esecuzione di dispositivi USB** sui sistemi aziendali.
Formare i dipendenti su **come comportarsi se trovano una chiavetta USB sospetta**.
Utilizzare **soluzioni di sicurezza endpoint** per bloccare dispositivi non autorizzati.

Raccomandazioni generali per l'azienda

- **Formazione e simulazioni periodiche** per tutti i dipendenti su social engineering.-
- **Creazione di una policy di sicurezza interna** chiara e accessibile.-
- **Monitoraggio attivo degli accessi e delle attività sospette** nei sistemi aziendali.-
- **Implementazione di sistemi di risposta agli incidenti (Incident Response Plan)** per reagire rapidamente a minacce.

CONCLUSIONE:

Il **social engineering** rappresenta una delle minacce più insidiose per aziende e individui, poiché sfrutta le debolezze umane più che le vulnerabilità tecniche. Gli attacchi analizzati dimostrano come la **mancanza di verifica dell'identità, l'accesso privilegiato e l'assenza di autenticazione a più fattori** possano facilitare intrusioni informatiche con gravi conseguenze economiche e reputazionali.

Per contrastare queste minacce, è essenziale adottare un approccio **proattivo**, basato su **formazione continua, politiche di sicurezza rigorose e strumenti di protezione avanzati**. Implementare **autenticazione a più fattori, controlli sugli accessi e simulazioni periodiche** può ridurre drasticamente il rischio di cadere vittima di attacchi di social engineering.

Analisi delle Vulnerabilità di Windows 10 e Strategie di Mitigazione

Windows 10, pur essendo uno dei sistemi operativi più utilizzati, presenta vulnerabilità critiche che possono essere sfruttate per **eseguire codice remoto, ottenere privilegi elevati o diffondere malware**.

Principali CVE Analizzate:

1- **CVE-2020-0796 (SMBGhost)** – Vulnerabilità nel protocollo **SMBv3**, permette esecuzione remota di codice e diffusione di ransomware.
Soluzione: Applicare la patch KB4551762, disabilitare SMBv3 e bloccare la porta 445.

2- **CVE-2021-34527 (PrintNightmare)** – Exploit nel servizio **Print Spooler**, consente escalation di privilegi e attacchi remoti.
Soluzione: Installare patch KB5004945, disabilitare Print Spooler su dispositivi non necessari.

3- **CVE-2019-0708 (BlueKeep)** – Vulnerabilità in **Remote Desktop Protocol (RDP)**, permette accesso non autenticato ai sistemi.
Soluzione: Applicare patch KB4499175, disabilitare RDP se non necessario, usare autenticazione a più fattori (MFA).

4-**CVE-2022-30190 ("Follina")** – Exploit in **Microsoft Office**, consente esecuzione di codice tramite documenti malevoli.
Soluzione: Applicare patch KB5015805, bloccare MSDT e non aprire allegati sospetti.

Misure di Protezione Generali:

✔ **Aggiornamenti regolari** con patch di sicurezza Microsoft.
✔ **Antivirus e firewall attivi** per monitorare attività sospette.
✔ **Autenticazione a più fattori (MFA)** per proteggere account critici.
✔ **Restrizioni sui permessi utente** per limitare accessi non autorizzati.
✔ **Backup frequenti** per prevenire danni da ransomware.

Conclusione: Identificare e mitigare le vulnerabilità di Windows 10 è essenziale per ridurre il rischio di attacchi. L'**applicazione tempestiva delle patch e l'adozione di buone pratiche di sicurezza** sono le migliori difese contro le minacce informatiche.