Cos’è e come prevenire un attacco Social Engineering

(fonte Chatgpt)

Richiesta a Chatgpt:

ChatGPT, potresti spiegare in modo molto esaustivo cos'è il social engineering e descrivere le tecniche più comuni utilizzate dagli attaccanti, come phishing e tailgating?

Una volta finito mi elenchi, sempre in modo esaustivo, anche alcune strategie efficaci per difendersi dagli attacchi di social engineering?

Risposta di Chatgpt:

Il **Social Engineering** è una tecnica utilizzata da malintenzionati per manipolare le persone al fine di ottenere informazioni riservate, accesso a sistemi protetti, o compiere azioni che potrebbero compromettere la sicurezza. A differenza degli attacchi che si basano su vulnerabilità tecniche (come malware o hacking), il social engineering si concentra sulla manipolazione psicologica e comportamentale delle persone. In sostanza, gli attaccanti sfruttano la fiducia, la curiosità, o la buona fede degli individui per ottenere ciò che vogliono.

Gli attacchi di social engineering sono generalmente indirizzati a sfruttare errori umani, come la mancanza di consapevolezza sulla sicurezza o una reazione impulsiva di fronte a una richiesta urgente.

### Tecniche Comuni di Social Engineering

**Phishing**

Il **Phishing** è una delle forme più comuni di attacco di social engineering, in cui l'attaccante cerca di ingannare la vittima facendole credere che una comunicazione provenga da una fonte affidabile, come una banca, una compagnia di carte di credito o un servizio di email. Il phishing viene tipicamente eseguito tramite email, SMS (smishing) o social media, e cerca di convincere la vittima a fare clic su un link dannoso o a fornire informazioni sensibili (ad esempio, nome utente, password, numero di carta di credito).

**Caratteristiche tipiche del phishing**:

* Email o messaggi con errori grammaticali o ortografici.
* Richieste urgenti, come il blocco di un account o la verifica di informazioni.
* Link sospetti che sembrano condurre a siti legittimi ma che sono in realtà falsi (URL falsificati).
* Allegati che contengono malware o software dannoso

**Esempio di phishing**: Un'email che sembra provenire da una banca che richiede di aggiornare il tuo account, con un link che ti reindirizza a una pagina di login falsa.

**Spear Phishing**

Il **Spear Phishing** è una forma più mirata di phishing in cui l'attaccante si concentra su un singolo individuo o una piccola azienda, raccogliendo informazioni specifiche per rendere l'attacco più convincente. Gli attacchi di spear phishing sono personalizzati e, spesso, sembrano provenire da una persona che la vittima conosce, come un collega o un superiore. A differenza del phishing generale, che è un attacco massivo, lo spear phishing è più mirato e difficile da rilevare.

**Caratteristiche tipiche del spear phishing**:

* Uso di informazioni personali (come nomi, titoli professionali, dettagli di lavoro).
* Messaggi che sembrano provenire da colleghi o partner di business.
* Richieste di azioni specifiche, come trasferimenti di denaro o download di file allegati.

**Pretexting**

Il **Pretexting** è una tecnica di social engineering in cui l'attaccante si finge qualcuno che la vittima conosce o una persona autorizzata a raccogliere informazioni. L'obiettivo è creare un pretesto credibile per raccogliere dati sensibili. Ad esempio, l'attaccante potrebbe fingersi un tecnico di supporto che ha bisogno di informazioni per risolvere un problema tecnico.

**Caratteristiche tipiche del pretexting**:

* La vittima viene contattata da qualcuno che ha una posizione o un ruolo che giustifica la richiesta di informazioni.
* L'attaccante potrebbe fare domande molto dettagliate per convincere la vittima che è parte di un processo legittimo.
* Utilizzo di informazioni raccolte precedentemente per sembrare più credibili.

**Esempio di pretexting**: Un attaccante si finge un dipendente di un'azienda di telecomunicazioni e chiede alla vittima il numero di carta di credito o altre informazioni personali, dicendo che c'è un problema con il suo servizio.

**Tailgating**

Il **Tailgating** è un tipo di attacco fisico di social engineering in cui un attaccante cerca di guadagnare accesso fisico a un'area protetta (come un edificio o un'area aziendale) seguendo una persona autorizzata senza che questa se ne accorga. L'attaccante sfrutta la cortesia della vittima, come tenere la porta aperta per una persona che sembra avere bisogno di aiuto.

**Caratteristiche tipiche del tailgating**:

* L'attaccante si avvicina a una persona autorizzata e cerca di entrare nello stesso edificio o area senza essere notato.
* Può fingere di essere un lavoratore temporaneo, un visitatore o qualcuno che ha dimenticato la propria tessera di accesso.
* Utilizzo di manovre psicologiche come la cortesia o la richiesta di aiuto per ottenere l'accesso non autorizzato.

**Esempio di tailgating**: Un individuo si avvicina a un dipendente che sta entrando nell'edificio e chiede di entrare con lui perché "ha dimenticato il badge di accesso". Il dipendente, vedendolo come una persona di passaggio, gli tiene aperta la porta.

**Baiting**

Il **Baiting** è una tecnica in cui l'attaccante offre qualcosa di attraente (come un download gratuito, un premio o una risorsa utile) per convincere la vittima a scaricare un file dannoso, a visitare un sito web infetto o a inserire informazioni sensibili. Il baiting sfrutta la curiosità naturale delle persone.

**Caratteristiche tipiche del baiting**:

* Offerta di qualcosa di gratuito o desiderabile (ad esempio, musica gratuita, software, premi).
* Utilizzo di dispositivi fisici (come chiavette USB infette) per distribuire malware.
* Promesse che attirano l'attenzione della vittima, ma che nascondono rischi.

**Esempio di baiting**: Un attaccante lascia una chiavetta USB infetta in un luogo pubblico, come un parcheggio, sperando che qualcuno la raccolga e la colleghi al proprio computer, infettando così il sistema.

**Strategie Efficaci per Difendersi dagli Attacchi di Social Engineering**

**Formazione e Consapevolezza**  
La formazione continua è fondamentale per sensibilizzare le persone sui rischi del social engineering. I dipendenti e gli utenti devono essere istruiti su come riconoscere i segnali di attacchi di social engineering, come email sospette, richieste non verificate o tentativi di accesso fisico non autorizzato. Formazioni periodiche e simulazioni di attacchi (ad esempio, phishing test) possono essere utili per migliorare la consapevolezza.

**Verifica delle Identità**  
È importante implementare procedure di verifica rigorose per qualsiasi richiesta di informazioni sensibili. Se qualcuno ti chiede informazioni riservate, verifica sempre la sua identità tramite un canale separato e sicuro. Non rispondere mai a richieste di informazioni via email o telefono senza aver prima verificato chi sta facendo la richiesta.

**Autenticazione Multi-Fattore (MFA)**  
L'uso di sistemi di autenticazione a più fattori rende molto più difficile per un attaccante accedere a account o sistemi protetti, anche se è riuscito a ottenere una password. La MFA richiede almeno due forme di autenticazione, come una password e un codice inviato via SMS o un'app di autenticazione.

**Politiche di Sicurezza Aziendale**  
Le aziende dovrebbero implementare politiche di sicurezza chiare, come limitare l'accesso fisico alle aree protette e l'accesso ai sistemi informatici solo a personale autorizzato. Inoltre, dovrebbero essere stabilite procedure chiare su come trattare le richieste di informazioni, come l'adozione di una politica di "non fornire mai informazioni a meno che non siano state verificate".

**Monitoraggio e Logging**  
Implementare un sistema di monitoraggio e registrazione delle attività sospette sia online che fisiche. Monitorare chi entra ed esce dai locali aziendali, registrare i dispositivi USB connessi a sistemi aziendali e tenere traccia delle attività online possono aiutare a rilevare rapidamente attività anomale

**Sospetta Sempre i Link e gli Allegati**  
Non fare mai clic su link sospetti, specialmente se provengono da email non richieste o da persone che non conosci. Assicurati sempre che l'URL sia legittimo e che il sito web sia sicuro (https://). Non aprire mai allegati da fonti sconosciute, poiché potrebbero contenere malware.

**Controllo degli Accessi**  
Utilizza il controllo degli accessi per garantire che solo le persone autorizzate abbiano accesso alle informazioni riservate o alle aree protette. Questo include l'uso di badge di accesso, controlli biometrici e dispositivi di blocco per impedire il tailgating.

**Gestione delle Credenziali**  
Incoraggia l'uso di password forti e uniche per ogni account. Utilizzare un gestore di password può aiutare a proteggere le credenziali. Inoltre, è importante cambiare regolarmente le password e disabilitare gli account inutilizzati.

In conclusione, il social engineering è una minaccia molto pericolosa poiché sfrutta la psicologia umana anziché la tecnologia. La protezione contro questi attacchi dipende dalla consapevolezza, dalla formazione e dall'adozione di misure preventive efficaci

**TRACCIA BONUS**

**Esplorazione dei CVE tramite ChatGPT**

**Richiesta a Chatgpt:**

Chat potresti fornirmi una lista dei CVE relativi a windows 10? Per ogni CVE mi occorre una lista estremamente dettagliata soprattutto mi occorrono i dettagli delle vulnerabilità e tutte le soluzioni consigliate

**Risposta di Chatgpt:**

Al momento non posso eseguire ricerche in tempo reale, quindi non posso fornirti una lista specifica di CVE relativi a Windows 10. Tuttavia, posso spiegarti come trovare queste informazioni e come interpretarle.

Per consultare dettagli relativi alle vulnerabilità (CVE) di Windows 10, puoi utilizzare le seguenti risorse:

**National Vulnerability Database (NVD)**: Una risorsa ufficiale degli Stati Uniti che contiene i dati delle vulnerabilità. Puoi cercare CVE specifici per Windows 10 filtrando per prodotto e versione.

* Sito web: [https://nvlpubs.nist.gov/nistpubs/](https://nvlpubs.nist.gov/nistpubs/" \t "_new)

**CVE Details**: Questo sito fornisce un elenco delle vulnerabilità CVE, inclusi dettagli sulle versioni e le risoluzioni. È utile per cercare vulnerabilità specifiche in Windows 10.

* Sito web: [https://www.cvedetails.com/](https://www.cvedetails.com/" \t "_new)

**Microsoft Security Advisories**: Microsoft pubblica aggiornamenti di sicurezza regolari che dettagliano vulnerabilità specifiche per Windows, compreso Windows 10.

* Sito web: [https://msrc.microsoft.com/](https://msrc.microsoft.com/" \t "_new)

**Struttura Tipica di un CVE**

Ogni record CVE include:

* **CVE ID**: Un identificatore unico per la vulnerabilità, ad esempio CVE-2024-XXXX.
* **Descrizione**: Una breve spiegazione del problema di sicurezza e come può essere sfruttato.
* **Severità**: Un punteggio che indica quanto è pericolosa la vulnerabilità, di solito espresso tramite il sistema **CVSS (Common Vulnerability Scoring System)**.
* **Soluzioni/Risorse**: Le raccomandazioni per risolvere la vulnerabilità, come aggiornamenti software, patch, o configurazioni consigliate.

Se desideri informazioni più dettagliate su un particolare CVE o sulla risoluzione di vulnerabilità di Windows 10, ti consiglio di consultare i siti sopra indicati, dove troverai tutte le informazioni complete.