RELAZIONE

Il **social engineering** è un insieme di tecniche manipolative utilizzate dagli attaccanti per ingannare le persone e ottenere informazioni riservate, accesso a sistemi protetti o altri vantaggi. A differenza degli attacchi informatici che sfruttano vulnerabilità tecniche, il social engineering si concentra sulla manipolazione psicologica delle persone, approfittando della loro fiducia, distrazione o ignoranza.

Tecniche comuni di social engineering:

1. **Phishing**:
    - Il phishing è una delle forme più comuni di social engineering, in cui l'attaccante si traveste da una fonte legittima (ad esempio una banca, un'azienda di servizi online o un amico) per ingannare la vittima. L'obiettivo è indurre la vittima a fornire informazioni sensibili, come credenziali di accesso, numeri di carte di credito, o altre informazioni personali.
    - Gli attacchi di phishing avvengono principalmente via email, ma possono essere realizzati anche tramite SMS (smishing) o chiamate telefoniche (vishing).
    - Esempio: un'email che sembra provenire da una banca, chiedendo di "confermare" i dati del conto, ma in realtà è un tentativo per rubare le credenziali dell'utente.
2. **Spear phishing**:
    - Una variante più mirata del phishing, il **spear phishing** si concentra su una persona o un'organizzazione specifica. Gli attaccanti possono raccogliere informazioni sulla vittima (ad esempio, tramite i social media) per rendere l'attacco più credibile e persuasivo.
    - Esempio: un'email che sembra provenire dal CEO di un'azienda, chiedendo a un dipendente di trasferire denaro o di fornire informazioni sensibili.
3. **Pretexting**:
    - Il pretexting implica la creazione di un falso pretesto o una storia per ottenere informazioni private. L'attaccante si inventa un'identità e un motivo credibile per richiedere dati sensibili.
    - Esempio: un attaccante si finge un dipendente del reparto IT e contatta un membro dell'azienda chiedendo le credenziali di accesso per risolvere un "problema tecnico".
4. **Baiting**:
    - Il baiting è un attacco che offre qualcosa di allettante in cambio di

informazioni sensibili o azioni specifiche. Può essere fisico (ad esempio, lasciare un dispositivo USB infetto in un luogo pubblico) o online (ad esempio, offrire un link a un software gratuito che in realtà è dannoso).
    - Esempio: un attaccante lascia una chiavetta USB con l'etichetta "Progetto segreto" in un'area pubblica, sperando che qualcuno la colleghi al proprio computer, innescando così l'installazione di malware.
5. **Tailgating** (o Piggybacking):
    - Il **tailgating** si riferisce all'atto di seguire un individuo legittimo all'interno di una zona protetta, come un edificio o un'area con accesso controllato, sfruttando la cortesia o l'inattenzione della vittima. L'attaccante non ha accesso fisico legittimo, ma riesce a entrare sfruttando la fiducia o l'errore di qualcun altro.
    - Esempio: un attaccante si avvicina a una persona che ha appena aperto una porta automatica di un ufficio e entra dietro di essa senza che la vittima se ne accorga.
6. **Quizzes e sondaggi falsi**:
    - Gli attaccanti utilizzano quiz e sondaggi online come mezzo per raccogliere informazioni personali. Le domande possono sembrare innocue (ad esempio, "Qual è il tuo primo animale domestico?") ma spesso sono usate per ottenere risposte a domande di sicurezza o altre informazioni utili.
    - Esempio: un attaccante crea un sondaggio su un social media chiedendo informazioni personali (come nome della madre, nome della prima scuola, ecc.) che vengono poi utilizzate per rispondere a domande di sicurezza su account bancari o social.

Come difendersi dal social engineering?

- **Educazione e consapevolezza**: La formazione regolare su come riconoscere e affrontare attacchi di social engineering è fondamentale.
- **Verifica delle comunicazioni**: Non fidarsi mai di una richiesta di informazioni sensibili senza confermare la sua autenticità.
- **Protezione delle informazioni personali**: Ridurre al minimo la quantità di informazioni personali condivise online.
- **Uso di autenticazione a due fattori (2FA)**: Questo aggiunge uno strato di protezione anche se le credenziali vengono compromesse.

Il social engineering sfrutta la psicologia umana, ed è per questo che rimane una delle minacce più efficaci. Essere vigili e prudenti nelle interazioni quotidiane è essenziale per proteggersi da questi attacchi.

Ecco alcune **strategie efficaci** per difendersi da questi attacchi:

1. Formazione e Consapevolezza

- **Educare i dipendenti e gli utenti**: La formazione è la prima linea di difesa. Le persone devono essere consapevoli delle tecniche di social engineering più comuni (ad esempio phishing, pretexting, baiting) e come riconoscerle. Educare i dipendenti su come riconoscere le e-mail sospette, come verificare richieste di informazioni e come rispondere in modo sicuro è cruciale.
- **Simulazioni di attacchi**: Eseguire simulazioni di attacchi di phishing e altre forme di social engineering può aiutare le persone a familiarizzare con queste minacce.
- **Spiegare ai dipendenti e agli utenti come riconoscere gli attacchi di social engineering**: Formare le persone su come individuare messaggi sospetti (email, telefonate, SMS, ecc.) che cercano di ottenere informazioni sensibili.
- **Corsi di sensibilizzazione**: Periodicamente, fare corsi e sessioni di aggiornamento sulla sicurezza informatica, specificando le minacce più comuni come il phishing, il vishing (phishing tramite telefonate), o il pretexting.

2. Verifica delle Identità

- **Controllo delle fonti**: Prima di divulgare qualsiasi informazione sensibile, è importante verificare l'identità del richiedente. Questo vale sia per le comunicazioni telefoniche che via e-mail. Se qualcuno afferma di essere una persona fidata, come un collega o un'autorità, è bene verificare tramite un canale diverso (ad esempio, chiamando il numero ufficiale o contattando il dipartimento pertinente).
- **Autenticazione a più fattori (MFA)**: Implementare l'autenticazione a più fattori (ad esempio, combinazione di password e un codice temporaneo inviato tramite SMS o un'app) per rendere più difficile l'accesso non autorizzato anche se le credenziali vengono compromesse.

3. Sospettare delle Richieste Urgenti

- **Non farsi prendere dal panico**: Gli attacchi di social engineering spesso cercano di creare un senso di urgenza o paura. Se una richiesta sembra troppo urgente o minacciosa (ad esempio, "La tua password sta per scadere, clicca qui subito per aggiornare"), è importante fare una pausa e valutare la situazione prima di rispondere.
- **Riflettere sulle richieste**: Se una richiesta sembra anomala o sospetta, è meglio fare una ricerca online o chiedere a qualcuno di più esperto prima di agire.

4. Protezione delle Informazioni Sensibili

- **Minimizzare la condivisione di informazioni**: Evitare di condividere informazioni personali, password, numeri di conto o altre informazioni sensibili su piattaforme pubbliche o in risposta a richieste non verificate.
- **Crittografia**: Proteggere i dati con crittografia, sia per la comunicazione via e-mail che per i file archiviati, per prevenire l'accesso non autorizzato.

5. Controllo degli Accessi

- **Principio del minimo privilegio**: Assicurarsi che ogni persona abbia accesso solo alle informazioni strettamente necessarie per il proprio ruolo. Questo riduce il rischio che un attaccante possa sfruttare un account compromesso per accedere a dati sensibili.
- **Monitoraggio e Audit**: Monitorare gli accessi e le attività degli utenti, in particolare per azioni sospette, può aiutare a rilevare comportamenti anomali e prevenire danni.

6. Difesa contro il Phishing

- **Non cliccare su link sospetti**: Le e-mail di phishing spesso contengono link che rimandano a siti falsi. È importante non cliccare su link o allegati sospetti e, se necessario, visitare i siti web direttamente digitando l'indirizzo nella barra del browser.
- **Verifica degli indirizzi e-mail**: Molti attacchi di phishing provengono da indirizzi e-mail che sembrano legittimi, ma che in realtà sono leggermente modificati. Verificare attentamente l'indirizzo dell'e-mail di origine può aiutare a riconoscere questi attacchi.

7. Sicurezza delle Password

- **Utilizzare password forti e uniche**: Evitare di usare la stessa password per più account. Utilizzare password complesse (combinazione di lettere maiuscole, minuscole, numeri e simboli) e cambiarle periodicamente.
- **Gestori di password**: Utilizzare un gestore di password per memorizzare in modo sicuro le credenziali e generare password forti.

8. Attenzione ai Social Media

- **Limitare le informazioni condivise**: Gli attaccanti utilizzano spesso le informazioni pubblicate sui social media per raccogliere dati e preparare attacchi mirati. È importante limitare la quantità di informazioni personali condivise e configurare i profili per massimizzare la privacy.
- **Privacy delle impostazioni sociali**: Impostare correttamente le impostazioni di privacy sui social network e fare attenzione a chi può visualizzare i contenuti

pubblicati.

9. Aggiornamento e Manutenzione della Sicurezza

- **Aggiornare regolarmente software e sistemi**: Assicurarsi che il sistema operativo, le applicazioni e i software di sicurezza siano sempre aggiornati per proteggersi contro le vulnerabilità.
- **Antivirus e firewall**: Utilizzare antivirus e firewall aggiornati per proteggere i dispositivi da malware che potrebbero essere utilizzati come parte di un attacco di social engineering.

10. Segnalazione di Attacchi

- **Segnalare attività sospette**: Se si sospetta di essere stati vittima di un attacco di social engineering, è fondamentale segnalarlo immediatamente al dipartimento di sicurezza informatica o ai responsabili della sicurezza dell'organizzazione.
- **Raccogliere prove**: Conservare i dettagli degli attacchi (come e-mail sospette, numeri di telefono o URL) per aiutare le forze dell'ordine o i team di sicurezza a investigare.

I **CVE (Common Vulnerabilities and Exposures)** sono identificatori univoci assegnati a vulnerabilità di sicurezza note nei software e nei sistemi informatici. Il sistema CVE è gestito dal **MITRE Corporation**, con il supporto di enti come il **NIST (National Institute of Standards and Technology)**, e serve a standardizzare la denominazione delle vulnerabilità per facilitarne la condivisione tra aziende, esperti di sicurezza e sviluppatori.

A cosa servono i CVE?

- Permettono alle aziende e ai professionisti della sicurezza di **comunicare e mitigare rapidamente** le vulnerabilità.
- Aiutano a **prioritizzare le patch** e gli aggiornamenti di sicurezza.
- Facilitano la **condivisione di informazioni** tra vendor, ricercatori e governi.

Ecco un elenco di alcune vulnerabilità note (CVE) relative a Windows 11, insieme a dettagli sulla natura della vulnerabilità e le soluzioni consigliate:

1. CVE-2023-50868

- **Descrizione**: Questa vulnerabilità riguarda un problema di tipo Denial of Service (DoS) nel processo di convalida DNSSEC. Un attaccante potrebbe sfruttare questa falla per causare un rapido esaurimento delle risorse della CPU, portando al crash del sistema.
- **Soluzione**: Microsoft ha rilasciato una patch nel giugno 2024 per correggere questa vulnerabilità. Si consiglia di aggiornare il sistema tramite Windows

Update per applicare la correzione.
cybersecurity360.it

2. CVE-2024-43451

- **Descrizione**: Si tratta di una vulnerabilità zero-day che è stata attivamente sfruttata in rete. I dettagli specifici sulla natura della vulnerabilità non sono stati divulgati pubblicamente.
- **Soluzione**: Microsoft ha incluso la correzione per questa vulnerabilità nel Patch Tuesday di novembre 2024. È fondamentale installare gli aggiornamenti più recenti tramite Windows Update per proteggere il sistema.
  cybersecurity360.it

3. CVE-2024-38081

- **Descrizione**: Questa vulnerabilità riguarda un'elevazione dei privilegi in .NET Framework su Windows 11. Un attaccante potrebbe sfruttare questa falla per eseguire codice con privilegi elevati.
- **Soluzione**: Microsoft ha rilasciato un aggiornamento cumulativo nel luglio 2024 per .NET Framework 3.5 e 4.8 su Windows 11 versione 21H2, che risolve questa vulnerabilità. È consigliabile installare questo aggiornamento tramite Windows Update.
  support.microsoft.com

4. CVE-2024-21302 (Downdate)

- **Descrizione**: Questa vulnerabilità sfrutta un difetto nel processo di installazione degli aggiornamenti di Windows. Durante una fase intermedia dell'installazione, viene creato un file (pending.xml) che potrebbe essere manipolato da un attaccante per eseguire codice non autorizzato.
- **Soluzione**: Per mitigare questa vulnerabilità, è essenziale applicare gli aggiornamenti di sicurezza rilasciati da Microsoft che affrontano questo specifico problema.
  kaspersky.it

5. CVE-2023-38146

- **Descrizione**: Questa vulnerabilità riguarda la funzione Temi di Windows. Un file tema appositamente creato potrebbe essere utilizzato per esfiltrare le credenziali NTLM dell'utente senza interazione diretta, semplicemente inducendo l'utente a visualizzare un'anteprima del tema dannoso.
- **Soluzione**: Microsoft ha rilasciato una patch per questa vulnerabilità nel settembre 2023. Inoltre, è possibile mitigare il rischio bloccando l'utilizzo dell'autenticazione NTLM tramite le policy di gruppo.

akamai.com

6. CVE-2022-26925

- **Descrizione**: Questa vulnerabilità riguarda l'autorità di sicurezza locale di Windows e può essere sfruttata in attacchi NTLM Relay contro i servizi certificati di Active Directory. Un attaccante potrebbe autenticarsi su un domain controller, ottenendo potenzialmente il controllo dell'intera rete.
- **Soluzione**: Microsoft ha rilasciato una patch per questa vulnerabilità nel maggio 2022. È fondamentale applicare questo aggiornamento e considerare l'implementazione di protezioni aggiuntive contro gli attacchi NTLM Relay. kaspersky.it

Per proteggere il tuo sistema Windows 11, è essenziale mantenere aggiornato il sistema operativo e applicare tempestivamente tutte le patch di sicurezza rilasciate da Microsoft. Utilizza Windows Update per assicurarti di avere gli aggiornamenti più recenti e considera l'implementazione di misure di sicurezza aggiuntive, come la limitazione dell'uso dell'autenticazione NTLM e la configurazione appropriata delle policy di gruppo.