Il **social engineering** è una tecnica che sfrutta la manipolazione psicologica per indurre le persone a compiere azioni o a rivelare informazioni riservate. Non si basa su exploit tecnologici, ma sull'inganno umano. Questo approccio è particolarmente efficace perché si concentra sulla vulnerabilità umana, come fiducia, curiosità, paura o distrazione.

Come funziona il social engineering?

Il social engineering può avvenire attraverso diversi mezzi, come telefono, email, social network o persino incontri di persona. L'obiettivo è far sì che la vittima compia un'azione desiderata, come fornire dati personali, cliccare su un link malevolo o dare accesso a sistemi informatici.

Tecniche comuni di social engineering

1. **Phishing**
    - Si tratta di email o messaggi falsi che sembrano provenire da fonti affidabili, come banche, servizi online o colleghi di lavoro.
    - L'email spesso contiene un link che porta a un sito web falso, progettato per rubare credenziali o altre informazioni.
2. **Spear Phishing**
    - Una versione più mirata del phishing, rivolta a un individuo o gruppo specifico. Gli attacchi sono personalizzati per sembrare più autentici.
3. **Pretexting**
    - Il malintenzionato crea una storia plausibile per convincere la vittima a fornire informazioni sensibili. Ad esempio, potrebbe fingere di essere un tecnico IT che ha bisogno di credenziali per "risolvere un problema".
4. **Baiting**
    - Si attira la vittima con un'esca, come un'unità USB infetta lasciata in un luogo pubblico con un'etichetta intrigante ("Dati riservati"). Quando viene collegata, l'attaccante ottiene accesso al sistema.
5. **Vishing (Voice Phishing)**
    - Simile al phishing, ma attraverso il telefono. L'attaccante può fingersi un operatore bancario, un agente di supporto tecnico o un rappresentante di un'azienda.
6. **Tailgating e Piggybacking**
    - L'attaccante entra fisicamente in un'area riservata seguendo un dipendente autorizzato. Spesso si approfitta della cortesia delle persone per ottenere accesso.
7. **Impersonation**
    - Il malintenzionato si presenta come una persona di fiducia, ad esempio un dirigente dell'azienda, per convincere il personale a seguire ordini non autorizzati.

Obiettivi principali

- **Dati personali**: numeri di carte di credito, password, informazioni di identificazione personale.
- **Accesso ai sistemi**: credenziali di login, autorizzazioni di rete.
- **Denaro**: truffe dirette o furti di informazioni per estorcere denaro.
- **Informazioni sensibili**: progetti aziendali, segreti industriali.

Come proteggersi dal social engineering?

1. **Educazione e consapevolezza**: Sapere cosa cercare e come riconoscere i tentativi di manipolazione.
2. **Autenticazione a più fattori (MFA)**: Anche se un malintenzionato ottiene una password, l'MFA può bloccare l'accesso.
3. **Verifica delle richieste**: Controlla sempre le richieste sospette con canali ufficiali.
4. **Non condividere informazioni personali**: Soprattutto via telefono o email non verificati.
5. **Politiche aziendali rigorose**: Le aziende dovrebbero implementare procedure per confermare richieste e limitare l'accesso ai dati sensibili.
6. **Diffida dell'urgenza**: Gli attacchi spesso sfruttano la pressione del tempo per indurti a commettere errori.

1. Phishing

Un attacco generico e molto diffuso.

- **Come funziona**: Viene inviata una comunicazione (email, messaggio di testo, ecc.) che sembra provenire da una fonte legittima. Spesso include un senso di urgenza per spingere la vittima a cliccare su un link o scaricare un allegato.
- **Esempio**:
  Una email che sembra provenire dalla tua banca con oggetto: *"Accesso al tuo conto sospeso"*. La mail include un link per "ripristinare l'accesso" che porta a una pagina web falsa progettata per raccogliere le tue credenziali.

2. Spear Phishing

Un tipo di phishing mirato, personalizzato per una specifica vittima o organizzazione.

- **Come funziona**: L'attaccante raccoglie informazioni sulla vittima (es. tramite social media o fonti pubbliche) e crea un messaggio altamente credibile.
- **Esempio**:
  - Un email personalizzata per un dirigente aziendale, apparentemente inviata dal CEO, che chiede con urgenza di trasferire denaro per un'operazione riservata.
  - Una mail a un dipendente con un allegato infetto dal titolo *"Piano di sviluppo aziendale 2024"*.

3. Pretexting

Il malintenzionato si costruisce una storia credibile per ottenere informazioni o accesso.

- **Come funziona**: Si finge una figura autorevole (tecnico IT, agente delle forze dell'ordine, dirigente aziendale) per ottenere fiducia.
- **Esempio**:
  - Qualcuno si presenta come tecnico IT e chiama un dipendente affermando che ci sono problemi con il suo account. Chiede username e password per "risolvere il problema".
  - Un malintenzionato chiama fingendosi della banca, chiedendo dettagli del conto per bloccare una transazione fraudolenta.

4. Baiting

Si attira la vittima con un'esca, promettendo qualcosa di interessante o utile, ma che nasconde un malware o una trappola.

- **Come funziona**: L'attaccante offre un incentivo o lascia qualcosa di intrigante a disposizione della vittima.
- **Esempio**:
  - Una chiavetta USB etichettata come *"Report Confidenziale"* lasciata in un luogo pubblico. Quando qualcuno la inserisce nel computer, viene installato un malware.
  - Un annuncio online che promette un software gratuito o uno sconto esclusivo, ma il link installa programmi malevoli.

5. Vishing (Voice Phishing)

Simile al phishing, ma si utilizza il telefono per ingannare la vittima.

- **Come funziona**: La vittima riceve una chiamata da qualcuno che si spaccia per un'autorità, un'azienda o un servizio fidato.
- **Esempio**:
  - Una chiamata da un falso operatore bancario che avverte di una "transazione sospetta" e richiede il codice OTP appena inviato.

- Un malintenzionato che si finge tecnico Microsoft e dice che il computer ha un virus, chiedendo accesso remoto per "risolvere il problema".

6. Smishing (SMS Phishing)

Attacco tramite messaggi di testo sul telefono.

- **Come funziona**: La vittima riceve un SMS che la invita a cliccare su un link o a fornire informazioni.
- **Esempio**:
  - Un messaggio che dice: *"La tua spedizione è bloccata, clicca qui per aggiornare i dati"* e il link porta a un sito truffa.
  - *"Hai vinto un premio! Rispondi con i tuoi dati per riscattarlo."*

7. Tailgating e Piggybacking

Tecniche fisiche per ottenere accesso a un'area riservata.

- **Come funziona**:
  - **Tailgating**: Il malintenzionato segue qualcuno autorizzato attraverso una porta di sicurezza, spesso approfittando della cortesia.
  - **Piggybacking**: L'attaccante chiede esplicitamente di essere fatto entrare, magari fingendosi un dipendente che ha dimenticato il badge.
- **Esempio**:
  - Un individuo sconosciuto entra dietro a un dipendente in un ufficio protetto, portando magari una scatola per sembrare un corriere.
  - Qualcuno con un aspetto professionale chiede al personale di reception di essere lasciato entrare senza badge.

8. Impersonation (Impersonificazione)

L'attaccante si finge una persona fidata o un'autorità.

- **Come funziona**: Si sfruttano dettagli reali (raccolti magari dai social network) per convincere la vittima della propria identità.
- **Esempio**:
  - Un malintenzionato si finge un dirigente aziendale e ordina a un dipendente di fornire accesso a documenti riservati.
  - Qualcuno si presenta come un tecnico esterno durante una manutenzione pianificata per entrare nei sistemi aziendali.

9. Quid Pro Quo

Offerta di un servizio o un vantaggio in cambio di informazioni.

- **Come funziona**: Il malintenzionato propone di aiutare la vittima in cambio di un'informazione o un'azione.
- **Esempio**:
  - Un finto tecnico chiama offrendo di risolvere un problema con il computer dell'azienda, ma chiede in cambio le credenziali.
  - Un attacco che promette una consulenza gratuita o un buono sconto se si completano alcuni moduli con informazioni personali.

Protezione contro il social engineering

1. **Non fidarti ciecamente**: Verifica sempre le richieste, specialmente quelle urgenti o non pianificate.
2. **Sii consapevole dei dettagli**: Controlla mittenti di email, URL di link e legittimità delle comunicazioni.
3. **Non fornire dati personali**: Specie a sconosciuti, via telefono o email.

4. **Controlla i dispositivi sconosciuti**: Non inserire USB o collegare dispositivi non verificati.
5. **Implementa protocolli aziendali**: Richiedi sempre verifiche in caso di ordini o richieste anomale.
6. **Formazione del personale**: Gli attacchi spesso puntano su dipendenti inconsapevoli o disattenti.

1. Educazione e consapevolezza

- **Come funziona**: I dipendenti e gli utenti devono essere formati per riconoscere i tentativi di manipolazione e comprendere i rischi del social engineering.
- **Esempi**:
    - **Formazione regolare**: Organizzare workshop aziendali per spiegare le tecniche di phishing, vishing e altre.
    - **Test simulati**: Inviare email di phishing simulate per testare la reazione dei dipendenti e correggere eventuali vulnerabilità.

2. Autenticazione a più fattori (MFA)

- **Come funziona**: Implementare sistemi di autenticazione che richiedano più passaggi per accedere a un account o sistema, come una password e un codice inviato al telefono.
- **Esempio**:
    - Anche se un attaccante ottiene una password tramite phishing, non potrà accedere senza il secondo fattore, come un codice SMS o una notifica push.

3. Verifica dell'identità su canali indipendenti

- **Come funziona**: Quando ricevi una richiesta sospetta, verifica l'identità della persona attraverso un canale alternativo (es. chiamandola direttamente a un numero ufficiale).
- **Esempio**:
    - Un email dal tuo "capo" richiede un trasferimento urgente di denaro. Prima di eseguire la richiesta, chiama il capo sul numero ufficiale per confermare.

4. Segnalare sospetti e anomalie

- **Come funziona**: Implementare un sistema semplice per segnalare email, telefonate o altre comunicazioni sospette all'interno dell'organizzazione.
- **Esempio**:
    - Un dipendente riceve un'email che sembra provenire dal reparto IT. Segnala il messaggio a un team di sicurezza interna prima di cliccare.

5. Limitare l'accesso ai dati sensibili

- **Come funziona**: Applicare il principio del *minimo privilegio*, consentendo l'accesso ai dati solo alle persone che ne hanno bisogno.
- **Esempio**:
    - In un'azienda, i dati finanziari sono accessibili solo al team contabile, rendendo più difficile per un attaccante ottenere informazioni tramite manipolazione di dipendenti di altri reparti.

6. Analisi delle email e controllo dei link

- **Come funziona**: Prestare attenzione ai dettagli di email sospette, come indirizzi email, errori grammaticali e link.
- **Esempio**:
    - Un'email da "amministrazione@b4nka.com" richiede informazioni personali. Controllando il dominio, ti accorgi che non appartiene alla tua banca ufficiale (banca.com).

7. Bloccare allegati e link sconosciuti

- **Come funziona**: Configurare i sistemi per filtrare automaticamente gli allegati sospetti o i link malevoli.
- **Esempio**:
    - Un sistema di sicurezza email può bloccare automaticamente i file .exe ricevuti via email o avvisarti se un link conduce a un sito non sicuro.

8. Politiche aziendali di verifica

- **Come funziona**: Creare protocolli chiari per gestire richieste sensibili o urgenti.
- **Esempio**:
    - Qualsiasi richiesta di trasferimento di denaro deve essere approvata da almeno due livelli di supervisione.

9. Non condividere informazioni sensibili sui social media

- **Come funziona**: Ridurre la quantità di informazioni personali disponibili online, che potrebbero essere sfruttate per attacchi mirati.
- **Esempio**:
    - Evitare di pubblicare dettagli sul lavoro, come il tuo ruolo o i nomi dei tuoi colleghi, per impedire agli attaccanti di utilizzare queste informazioni nei loro pretexting.

10. Monitoraggio continuo delle attività sospette

- **Come funziona**: Utilizzare strumenti di monitoraggio e analisi per identificare attività insolite sui sistemi aziendali.
- **Esempio**:
    - Un dipendente tenta di accedere a file sensibili fuori dal suo normale orario lavorativo. Il sistema invia una notifica al team di sicurezza.

11. Politiche di password forti e sicure

- **Come funziona**: Obbligare l'uso di password complesse, uniche e la loro regolare modifica.
- **Esempio**:
    - Una password come *Pa$$w0rd123* è debole; una più sicura potrebbe essere *Jm@82t!Qk$X*. Inoltre, mai usare la stessa password su più piattaforme.

12. Educazione sull'urgenza

- **Come funziona**: Gli attacchi di social engineering spesso creano un senso di urgenza per far agire le vittime senza pensare. Formare le persone a riconoscere e reagire correttamente.
- **Esempio**:
    - Una chiamata che dice: *"Se non risolvi questo problema entro 10 minuti, il tuo conto sarà bloccato!"*. Gli utenti dovrebbero sapere che le aziende legittime non operano in questo modo.

13. Evitare l'uso di dispositivi sconosciuti

- **Come funziona**: Non utilizzare chiavette USB, dispositivi o software che non provengano da fonti affidabili.
- **Esempio**:
    - Una chiavetta trovata in un parcheggio potrebbe essere un'esca. Inserendola nel computer aziendale, potresti attivare un malware.

14. Simulazioni e audit periodici

- **Come funziona**: Condurre audit regolari della sicurezza e simulazioni di attacchi per verificare la prontezza dei dipendenti.
- **Esempio**:
    - Un'azienda potrebbe simulare un attacco di phishing interno per vedere se i dipendenti segnalano l'email o cliccano sul link.

15. Cultura della sicurezza collaborativa

- **Come funziona**: Incoraggiare un ambiente in cui i dipendenti si sentano responsabili e collaborativi nella protezione dei dati.
- **Esempio**:
    - Premiare i dipendenti che individuano e segnalano tentativi di social engineering, creando una cultura positiva.

Windows 10 ha ricevuto numerosi CVE (Common Vulnerabilities and Exposures) relativi a falle di sicurezza. Ecco un elenco di alcuni esempi significativi e le relative strategie di mitigazione:

Esempi di CVE e Dettagli

1. CVE-2024-43491

- **Descrizione**: Questa vulnerabilità nella *Servicing Stack* ha reintrodotto falle precedentemente mitigate su Windows 10 versione 1507 (Enterprise 2015 LTSB e IoT Enterprise). Gli aggiornamenti distribuiti tra marzo e agosto 2024 hanno portato al ripristino involontario di vecchie vulnerabilità.
- **Impatto**: Potenziale esecuzione di codice arbitrario sfruttando componenti opzionali.
- **Soluzione**:
    - Applicare **l'aggiornamento di settembre 2024 alla Servicing Stack (SSU KB5043936)**.
    - Installare successivamente l'**aggiornamento di sicurezza KB5043083**【11†source】【14†source】.

2. CVE-2023-38541

- **Descrizione**: Problemi di permessi ereditati in alcuni driver Intel HID Event Filter su Windows 10 hanno permesso a utenti autenticati di ottenere privilegi elevati.
- **Impatto**: Escalation dei privilegi tramite accesso locale.
- **Soluzione**: Aggiornare i driver Intel HID Event Filter alla versione 2.2.2.1 o successiva【12†source】.

3. CVE-2023-34642

- **Descrizione**: Vulnerabilità in *KioWare for Windows*, fino alla versione 8.33, consentiva agli attaccanti di aprire una finestra di comando senza privilegi adeguati.
- **Impatto**: Abuso del comando showDirectoryPicker() per eseguire comandi in modalità non autorizzata.
- **Soluzione**: Aggiornare a versioni successive di *KioWare for Windows* per applicare i filtri corretti alle finestre di dialogo【11†source】.

Strategie di Mitigazione Generale

1. **Aggiornamenti Regolari**:
    - Installare sempre le patch di sicurezza distribuite da Microsoft.
    - Abilitare gli aggiornamenti automatici per ricevere correzioni tempestive.

2. **Controllo dei Permessi**:
    - Limitare i privilegi degli utenti per ridurre i rischi di escalation.
    - Controllare e aggiornare regolarmente i driver e i software di terze parti.
3. **Monitoraggio della Rete e dei Sistemi**:
    - Implementare soluzioni di monitoraggio per rilevare comportamenti sospetti o anomali.
    - Usare strumenti di analisi del traffico per identificare attacchi in tempo reale.
4. **Segmentazione della Rete**:
    - Ridurre il rischio di diffusione di attacchi segmentando la rete in sottoreti più sicure.
5. **Formazione degli Utenti**:
    - Educare gli utenti a riconoscere comportamenti anomali o tentativi di phishing.

Dettagli della vulnerabilità

- **Origine del problema**:
  I driver Intel HID Event Filter (utilizzati per gestire input da dispositivi hardware, come tastiere o pulsanti specifici) non gestivano correttamente i permessi. Questo ha permesso a utenti autenticati (ma con privilegi limitati) di sfruttare questa vulnerabilità per ottenere diritti amministrativi sul sistema.
- **Impatto**:
  Gli aggressori possono eseguire codice o compiere operazioni critiche sfruttando i permessi elevati, compromettendo il sistema o accedendo a dati riservati.

Esempio pratico

Un utente malintenzionato interno a un'azienda, con accesso a un dispositivo Windows 10 vulnerabile, sfrutta un'applicazione o un comando che utilizza il driver Intel per eseguire un'escalation dei privilegi. Questo potrebbe consentirgli di installare software non autorizzati, alterare configurazioni di sistema o accedere a dati protetti.

Soluzione

- **Aggiornamento del driver**:
  Intel ha rilasciato un aggiornamento che risolve la vulnerabilità. La versione sicura è **2.2.2.1 o successive**.
- **Come procedere**:
    1. Scaricare e installare l'aggiornamento dal sito ufficiale di Intel o tramite Windows Update.
    2. Verificare che tutti i driver siano aggiornati periodicamente.

Misure preventive aggiuntive

1. **Limitare i privilegi degli utenti**: Anche se un account viene compromesso, dovrebbe avere accesso solo a risorse non critiche.
2. **Monitoraggio**: Utilizzare strumenti di rilevamento delle anomalie per identificare tentativi di escalation.

Questa vulnerabilità evidenzia l'importanza di mantenere aggiornati tutti i componenti del sistema, inclusi i driver di terze parti.

RIASSUNTO

1. Cos'è il Social Engineering

- **Definizione**: È una tecnica di manipolazione psicologica usata per indurre una persona a condividere informazioni sensibili o compiere azioni che favoriscono un attacco.
- **Tecniche comuni**:
  - *Phishing*: Email fraudolente per ottenere credenziali.
  - *Pretexting*: Creare scenari falsi per rubare dati.
  - *Baiting*: Offrire incentivi (es. chiavette USB infette).
  - *Tailgating*: Accedere fisicamente a spazi riservati seguendo qualcuno.
- **Obiettivo**: Rubare dati personali, installare malware o compromettere sistemi aziendali.

2. Difese contro il Social Engineering

- **Formazione**: Sensibilizzare gli utenti sui rischi e sulle tecniche comuni.
- **Autenticazione robusta**: Implementare l'autenticazione a due fattori (2FA).
- **Verifiche di sicurezza**: Verificare le richieste sospette con metodi indipendenti.
- **Monitoraggio continuo**: Utilizzare strumenti per rilevare comportamenti anomali.
- **Simulazioni di attacchi**: Testare la reazione dei dipendenti con esercitazioni di phishing.

3. CVE relativi a Windows 10

- **CVE-2024-43491**:
  - Vulnerabilità nella *Servicing Stack* di Windows 10 versione 1507.
  - **Rimedio**: Applicare gli aggiornamenti SSU KB5043936 e KB5043083.
- **CVE-2023-38541**:
  - Problema nei driver Intel HID Event Filter che consente escalation di privilegi.
  - **Rimedio**: Aggiornare i driver alla versione 2.2.2.1 o successiva.
- **Strategie generali**:
  - Installare regolarmente le patch.
  - Limitare i privilegi degli utenti.
  - Monitorare la rete per attività sospette.

4. Controllo dei permessi (esempio approfondito)

- **Scopo**: Limitare l’accesso ai dati e alle risorse in base al ruolo dell’utente.
- **Applicazione**:
  - *Role-Based Access Control (RBAC)*: Configurare gli accessi in base ai ruoli aziendali.
  - Limitare l'uso di account amministrativi solo per operazioni critiche.
- **Esempio pratico**: Nel caso di CVE-2023-38541, gli utenti senza controllo dei permessi potrebbero sfruttare driver vulnerabili per ottenere privilegi di amministrazione.