Federico
Cuccu

Social Engineering: Tecniche, Esempi e Difese

Come proteggere dati e sistemi dalle minacce del social engineering nel 2024

Obiettivi della presentazione

- Comprendere cos'è il social engineering e perché è una minaccia crescente
- Esplorare le tecniche di attacco più diffuse nel 2024
- Analizzare esempi realistici di ogni tecnica
- Apprendere le difese e le best practice contro questi attacchi

Anche il contenuto della presentazione è stato generato da chatgpt, a scopo di esercizio.
Link alla chat intera: **CLICCA QUI**

Cos'è il Social Engineering?

Il social engineering è un insieme di **tecniche manipolative** utilizzate per ingannare le persone e ottenere informazioni sensibili o accesso non autorizzato a sistemi e dati.

L’obiettivo degli attaccanti è:

- rubare credenziali
- accedere a sistemi interni
- sottrarre denaro
- sottrarre informazioni riservate.

Perché il Social Engineering è una Minaccia Maggiore nel 2024

- **Sofisticazione degli attacchi**: Utilizzo di AI, Big Data e tecnologie come i deepfake.
- **Maggiore esposizione dei dati personali**: I social media e la condivisione online offrono agli attaccanti numerose informazioni per personalizzare gli attacchi.
- **Costo per le aziende**: Violazioni di dati, perdite finanziarie, danni alla reputazione e costi di ripristino.

Tecniche più diffuse di Social Engineering nel 2024

- Phishing avanzato
- Vishing e Smishing (Voice e SMS Phishing)
- Impersonificazione sui social media
- Pretexting (Pretesto)
- Baiting (Esca)
- Attacchi via QR Code
- Deepfake e Video Call Phishing

Esempi di social engineering

Esempio di Phishing Avanzato

Un dipendente di una grande azienda riceve un’email apparentemente da un fornitore di fiducia, che include dettagli precisi sui loro ultimi ordini.

L’email sembra legittima e chiede al destinatario di cliccare su un link per “verificare la fattura” o “aggiornare il metodo di pagamento”.

La pagina di accesso a cui conduce è una copia del sito ufficiale, progettata per **rubare le credenziali aziendali** del dipendente.

Scopo: Rubare le credenziali del dipendente per accedere a risorse aziendali, come l’ERP o i dati finanziari.

Esempio di Vishing

Un impiegato riceve una chiamata da una persona che si spaccia per un membro del dipartimento IT dell'azienda.

Il finto operatore comunica all'impiegato che ci sono stati tentativi di accesso non autorizzati al suo account aziendale e che serve verificare l'identità tramite l'inserimento di un codice inviato via SMS.

Tuttavia, il codice è in realtà un codice OTP (One-Time Password) inviato per **confermare una transazione fraudolenta**.

Scopo: Autorizzare transazioni o modificare credenziali di accesso, ottenendo così l'accesso a risorse aziendali sensibili.

Esempio di impersonificazione sui social media

Un attaccante crea un **profilo falso** di un manager aziendale su LinkedIn o Facebook, utilizzando foto e dettagli personali accessibili pubblicamente.

Poi invia un messaggio a un dipendente, richiedendo **“in via confidenziale”** informazioni su alcuni progetti in corso o chiedendo un aiuto finanziario temporaneo, suggerendo che non è stato possibile accedere a fondi aziendali.

Scopo: Estrarre informazioni riservate sui progetti in corso o sottrarre denaro con pretesti credibili.

Esempio di Pretexting (Pretesto)

Un attaccante si presenta come un rappresentante dell’assistenza clienti del fornitore di servizi IT della vittima, chiamando l’ufficio e dicendo di dover aggiornare i server.

Per “verificare” le impostazioni attuali, chiede alla vittima le **credenziali di accesso** e **l’indirizzo IP**. La vittima, credendo sia una normale procedura, fornisce le informazioni.

Scopo: Ottenere l’accesso ai sistemi aziendali per rubare dati sensibili o installare malware.

Esempio di Baiting (Esca)

In un ufficio frequentato da dipendenti aziendali, un attaccante lascia una **chiavetta USB** con un’etichetta invitante come “Documenti finanziari” o “Rapporto sui bonus”.

La chiavetta contiene **malware** che infetta il computer non appena inserita, dando accesso all'attaccante alla rete aziendale.

Scopo: Infiltrare malware nella rete aziendale per esfiltrare dati, installare ransomware o ottenere accessi non autorizzati.

Esempio di attacchi via QR Code

Un attaccante applica un **falso QR** code sopra quello reale su una locandina di un evento aziendale o in un ristorante frequentato da impiegati dell'azienda target.

Il QR code indirizza le vittime a una **pagina di login finta** che replica il portale di un servizio comunemente usato, come Microsoft 365, per rubare le credenziali.

Scopo: Raccogliere credenziali di accesso per sfruttarle in un attacco successivo o venderle sul mercato nero.

Esempio di Deepfake e Video Call Phishing

Un dipendente del settore finanziario riceve una videochiamata apparentemente dal proprio direttore finanziario (CFO), che chiede con urgenza di **autorizzare un pagamento** verso un nuovo fornitore.

Il deepfake è realistico, e l'urgenza convincente. Senza dubitare, il dipendente procede con la transazione.

Scopo: Indurre la vittima ad autorizzare un pagamento verso un conto controllato dall'attaccante.

Sistemi di difesa

Difese contro il Phishing avanzato

- **Autenticazione Multi-Fattore (MFA)**: Anche se un attaccante riesce a rubare le credenziali, l'uso di MFA rende più difficile il login, poiché richiede un secondo fattore di autenticazione.

- **Software di rilevamento del phishing**: I sistemi di e-mail aziendali dovrebbero includere un filtro anti-phishing avanzato, spesso basato sull'intelligenza artificiale, che analizza il contenuto, il mittente e gli allegati.

- **Politiche di verifica esterna dei link**: I dipendenti dovrebbero essere istruiti a verificare la destinazione di link sospetti e a evitare di inserire dati sensibili su pagine aperte da e-mail non verificate.

Difese contro il Vishing e Smishing

- **Politiche di verifica delle chiamate**: La formazione aziendale dovrebbe includere una politica che vieta di fornire informazioni sensibili su richiesta telefonica senza un protocollo di verifica dell'identità.

- **Protezione dei numeri aziendali e personali**: Limitare la diffusione dei numeri di telefono aziendali pubblicamente e informare i dipendenti sui rischi degli attacchi tramite SMS.

- **Autenticazione Out-of-Band**: Quando richiesto, confermare le richieste tramite un canale differente (ad esempio, email o tramite un'app aziendale sicura) per evitare che un attaccante possa condurre attacchi tramite telefonia.

Difese contro l’Impersonificazione sui social media

- **Monitoraggio dei social media aziendali**: Usare strumenti di monitoraggio per rilevare eventuali account falsi e segnalarli alle piattaforme.

- **Separazione delle informazioni personali e aziendali**: Incoraggiare i dipendenti a non pubblicare dettagli aziendali o relazioni di lavoro sui social, riducendo le informazioni a disposizione degli attaccanti.

- **Verifiche interne per richieste non abituali**: Se si riceve una richiesta di informazioni riservate o finanziarie, anche da colleghi conosciuti, è buona pratica verificarla direttamente con la persona, senza utilizzare i social media.

Difese contro il Pretexting

- **Politiche di autenticazione delle richieste interne**: Implementare protocolli di verifica interni per tutte le richieste di informazioni sensibili, soprattutto se provengono da fonti esterne o inusuali.

- **Autenticazione Multi-Fattore per accesso ai dati critici**: Rendere obbligatorio l'uso di MFA per accedere a dati e risorse aziendali di alto valore.

- **Consapevolezza del “principio del minimo privilegio”**: Limitare l'accesso ai dati aziendali solo ai dipendenti che ne hanno effettivamente bisogno e sensibilizzare sull’importanza di non condividere informazioni al di fuori dei canali aziendali.

Difese contro il Baiting

- **Bloccare l'accesso automatico a dispositivi esterni**: Disabilitare il riconoscimento automatico di chiavette USB nei computer aziendali e richiedere che siano prima verificate tramite strumenti di sicurezza IT.

- **Campagne di sensibilizzazione sul rischio dei dispositivi sconosciuti**: Educare i dipendenti sui rischi di connettere dispositivi esterni non autorizzati e spiegare come verificare l’autenticità di un dispositivo.

- **Software di sicurezza endpoint**: Implementare soluzioni di protezione avanzata sugli endpoint (computer aziendali) per rilevare malware e attività sospette in caso di collegamento di dispositivi esterni.

Difese contro gli Attacchi via QR Code

- **Verifica manuale dei QR code**: Educare i dipendenti a verificare l'autenticità dei QR code, se possibile, accedendo al sito web dell'azienda direttamente tramite il browser invece di usare il QR code.

- **Scanner QR con protezione anti-phishing**: Fornire app per la scansione dei QR code con protezioni integrate contro i link malevoli.

- **Distribuzione sicura dei QR code aziendali**: Garantire che i QR code aziendali siano affissi in luoghi protetti e difficili da manomettere, evitando di posizionarli in luoghi pubblici o poco sorvegliati.

Difese contro i Deepfake e il Video Call Phishing

- **Verifica multi-fattoriale per richieste finanziarie**: Ogni richiesta di transazione dovrebbe richiedere conferme tramite più canali e coinvolgere più di una persona autorizzata per la verifica.

- **Utilizzo di tecnologie di rilevamento dei deepfake**: In caso di comunicazioni altamente sensibili, utilizzare software avanzati in grado di rilevare manipolazioni video e audio.

- **Politiche di riconferma interna**: Implementare una policy per verificare tutte le richieste di trasferimenti finanziari con il richiedente tramite un canale sicuro e diretto, come una chiamata telefonica.

Conclusioni

Conclusioni

Queste misure difensive, in combinazione con una solida cultura di sicurezza informatica, offrono un alto livello di protezione contro gli attacchi di social engineering e **riducono significativamente il rischio di compromissione** dei sistemi e delle informazioni aziendali.

In sintesi:

- Le tecniche di social engineering utilizzate dagli attaccanti sfruttano le **vulnerabilità umane** per accedere a dati e sistemi.
- Come strategie di difesa, combina **tecnologie di sicurezza avanzate** con **consapevolezza** e **formazione**.
- Come best practice, monitora le tendenze e **aggiorna le misure di difesa** continuamente.