Attacchi di social engineering basati su AI: proteggere i dati e restare conformi

In questa prima parte della nostra serie di blog dedicata agli studi clinici, esploriamo alcune delle priL'intelligenza artificiale sta rapidamente trasformando il modo in cui i cyber-criminali conducono attacchi informatici. In questo blog tratteremo di come l'AI stia rendendo il social engineering (ingegneria sociale) più difficile da rilevare, l'impatto sui settori ad alto valore e i passi concreti che le organizzazioni possono adottare per ridurre il rischio.

Oggi gli strumenti di AI consentono agli attaccanti di lanciare frodi su larga scala, raccogliere dettagli personali per attacchi mirati e impersonare dirigenti con deepfake estremamente convincenti. Il risultato è un aumento degli attacchi, più difficili da individuare e con conseguenze finanziarie, giuridiche e reputazionali sempre più gravi.

Approfondiremo ciascuna di queste aree:

- Cos'è il social engineering
- Le 4 fasi di un attacco di social engineering
- Come l'AI rende il social engineering più difficile da rilevare
- Come difendere la propria organizzazione dal social engineering

Cos'è il social engineering o ingegneria sociale?

Il social engineering è una forma di manipolazione criminale attraverso la quale gli attaccanti sfruttano la psicologia umana invece di violare i sistemi tecnici. Invece di forzare vulnerabilità software, raccolgono informazioni e creano un rapporto fiduciario per generare una falsa percezione di familiarità o legittimazione.

Questa strategia manipolatoria permette loro di indurre le vittime a rivelare informazioni riservate o concedere accesso a sistemi protetti.

La maggior parte degli attacchi segue quattro fasi chiave, progettate per sfruttare il comportamento umano e la naturale propensione alla fiducia e alla collaborazione.

In ogni fase, i social engineer utilizzano leve psicologiche come autorità, urgenza e curiosità. L'attacco appare meno come un "hacking" e più come una conversazione, motivo per cui risulta così pericoloso. Per i vertici aziendali, la preoccupazione è che questi attacchi abbiano successo nonostante ingenti investimenti in strumenti di cybersecurity.

Le 4 fasi di un attacco di social engineering

1. **Raccolta di informazioni**

Gli attaccanti raccolgono dettagli su dipendenti, fornitori e dirigenti per costruire approcci credibili. Può bastare una ricerca su LinkedIn per i ruoli aziendali, un'occhiata al sito web per eventi imminenti o l'analisi del formato delle e-mail. Altri cercano sui social media compleanni, hobby o familiari. Alcuni arrivano a scandagliare il dark web o documenti cartacei scartati per reperire dati sensibili.

Esempio: un attaccante vede su LinkedIn che l'azienda ha assunto nuovo personale. Sapendo dal sito web che l'IT usa un formato standard di e-mail, prepara un messaggio convincente fingendosi helpdesk.

Suggerimento: ricordare regolarmente ai nuovi dipendenti, durante l'onboarding, che l'IT non richiede mai password o dati personali via email. Rinforzare questo messaggio anche presso tutta la forza lavoro.

2. **Costruzione della fiducia**

Con le informazioni raccolte, gli attaccanti si spacciano per colleghi, fornitori o autorità. Possono utilizzare pretexting (fingersi un fornitore o un autorità di controllo) o baiting (offrire risorse autentiche per conquistare la fiducia). Possono connettersi su LinkedIn, fare seguito a un invito a un evento o impersonare l'assistenza tecnica.

Esempio: l'attaccante chiama un dipendente fingendosi un tecnico IT. Cita le recenti assunzioni e spiega che stanno effettuando un reset password per risolvere problemi di accesso.

Suggerimento: incoraggiare i dipendenti a verificare le comunicazioni inaspettate, soprattutto se richiedono azioni, tramite un secondo canale (telefonata a un numero noto, verifica su directory interna, passphrase concordate).

3. **Sfruttamento**

Una volta costruita la fiducia, l'attaccante formula una piccola richiesta che abbassa le difese. Spesso ciò avviene tramite phishing o spear phishing (e-mail con link, allegati o richieste di login), oppure tramite vishing e smishing (truffe via telefono o SMS) con toni urgenti e pressanti. Queste richieste possono presto portare a concessioni molto più delicate e gravi.

Esempio: il "tecnico" invia al dipendente un link a una falsa pagina di login e chiede di inserire username e password per testare il sistema.

Suggerimento: formare i dipendenti a esaminare criticamente le e-mail. Controllare l'indirizzo del mittente al fine di individuare possibili errori minimi o nascosti, passare il cursore sui link per vedere la destinazione reale e dubitare di messaggi pressanti per ragioni di urgenza o che manifestano segretezza.

4. **Esecuzione**

Infine, l'attaccante incassa. Questo può significare rubare dati, installare malware o, più spesso, compiere frodi finanziarie.

Esempio: con le credenziali rubate, l'attaccante accede ai sistemi interni, scarica file riservati e utilizza l'account compromesso per lanciare ulteriori phishing dall'interno dell'organizzazione.

Suggerimento: segmentare i diritti di accesso così che, anche se un account viene compromesso, l'attaccante non possa muoversi liberamente. Applicare il principio del "least privilege" e verificare regolarmente chi ha accesso a cosa.

In che modo l'AI rende il social engineering più difficile da rilevare

L'AI non ha inventato nuove forme di social engineering: phishing, contraffazione e richieste fraudolente restano le tattiche principali. Ciò che è cambiato è scala, velocità e credibilità.

Secondo Tech News, nel 2025 gli attacchi informatici basati su AI sono cresciuti del 47% a livello globale. Un singolo messaggio convincente, una fattura falsa, una richiesta da un'autorità amministrativa o di

controllo o un dirigente impersonato, può superare le difese tradizionali e causare gravi danni economici, giuridici e reputazionali.

Per i vertici aziendali, questo significa che il social engineering non è più solo un problema IT, ma un rischio strategico da affrontare a livello di board.

Esempi di come l'AI sta ridefinendo le truffe:

- **Polished Phishing**: email e messaggi generati da AI, privi di errori grammaticali, contestualizzati e coerenti con il tono aziendale, che eliminano i segnali d'allarme tradizionali.
- **Deepfake di imitazione**: clonazione vocale e video alimentata da AI, in grado di imitare dirigenti, colleghi o regolatori in scenari ad alta pressione (pagamenti urgenti, richieste di dati).
- **Ricognizione automatizzata**: scraping di social media, siti web e registri pubblici per creare profili dettagliati delle vittime.
- **Truffe adattive**: chatbot AI che interagiscono in tempo reale, adattando le risposte a dubbi o esitazioni e rendendo la truffa naturale e non artefatta.
- **Scala e velocità**: migliaia di truffe personalizzate generate contemporaneamente, ciascuna leggermente diversa, in grado di soggiogare gli utenti e superare gli strumenti di sicurezza tradizionali.

Difendere la propria organizzazione dagli attacchi di social engineering

Contrastare minacce potenziate dall'AI richiede più di una singola soluzione. Serve un approccio a più livelli che combini persone, tecnologia e processi chiari.

1. **Rafforzare la consapevolezza del personale**
   Formazione continua sulle tattiche di social engineering, mostrando come gli attaccanti sfruttino urgenza, autorità e paura. Promuovere una cultura del "fermarsi e verificare".
2. **Eseguire simulazioni di phishing**
   Testare la prontezza con esercitazioni realistiche che aiutino a riconoscere e gestire messaggi sospetti in un contesto sicuro.
3. **Implementare filtri email intelligenti**
   Bloccare domini falsificati, allegati malevoli e link sospetti prima che raggiungano le caselle di posta. Integrare sistemi di anomaly detection (rilevamento di anomalie).
4. **Richiedere l'autenticazione a più fattori (MFA)**
   Rendere obbligatoria un sistema di MFA resistente al phishing su tutti gli account per prevenire violazioni anche in caso di credenziali compromesse.
5. **Aggiornare regolarmente le procedure**
   Mantenere le procedure di sicurezza e gestione dei dati allineate alle minacce in evoluzione. Avere un piano di risposta agli incidenti ben definito.
6. **Ridurre la superficie di attacco**
   Limitare le informazioni aziendali pubbliche e incoraggiare i dipendenti a rafforzare le impostazioni di privacy su social e reti professionali.

Conclusioni

L'AI sta trasformando il social engineering in una minaccia più veloce, scalabile ed efficace. Un'unica e-mail di phishing o una chiamata deepfake può causare perdite finanziarie rilevanti, sanzioni amministrative e danni reputazionali duraturi.

I settori ad alto valore, Finanziario, Life Sciences e IT, ne stanno già subendo le conseguenze.

Gli strumenti tradizionali da soli non bastano più. È essenziale una difesa multilivello che combini formazione del personale, procedure chiare e soluzioni tecniche avanzate, riducendo al contempo l'impronta digitale dell'organizzazione.

Incorporando consapevolezza e resilienza in persone, processi e tecnologia, le aziende possono ridurre l'esposizione e mantenere la fiducia di clienti, autorità e stakeholder.

Se la tua organizzazione desidera avvalersi di una consulenza specializzata in materia di protezione dei dati e sicurezza, contattaci per scoprire come i nostri servizi di DPO in outsourcing possano supportare e rafforzare il tuo business.