Social Engineering: Tecniche e Difese

Introduzione al Social Engineering

Il social engineering è l'arte di manipolare le persone per ottenere informazioni o eseguire azioni che potrebbero compromettere la sicurezza. Queste tecniche sfruttano la fiducia, la paura e la curiosità delle vittime per raggiungere scopi malevoli.

Tecniche Tradizionali di Social Engineering e Difese

Phishing

Descrizione: Invio di e-mail o messaggi per ingannare la vittima a rivelare informazioni.

Difese: Utilizzare software anti-phishing, non cliccare su link sospetti, verificare sempre la provenienza delle email.

Spear Phishing

Descrizione: Phishing mirato a una persona o azienda specifica.

Difese: Implementare procedure di verifica multi-fattoriale, educare il personale sui rischi specifici.

Pretexting

Descrizione: Creare un falso pretesto per ottenere informazioni.

Difese: Verificare l'identità della persona prima di rilasciare informazioni, seguire le politiche aziendali.

Baiting

Descrizione: Offerta di qualcosa di allettante (come una USB infetta) per accedere ai dati.

Difese: Non inserire dispositivi sconosciuti nel proprio computer, utilizzare soluzioni di sicurezza che bloccano l'esecuzione di malware.

Quid Pro Quo

Descrizione: Scambio di informazioni in cambio di un vantaggio.

Difese: Diffidare di richieste non sollecitate di assistenza, verificare sempre l'identità di chi offre aiuto.

Tailgating

Descrizione: Seguire qualcuno in un'area riservata senza autorizzazione.

Difese: Educare il personale a non permettere l'ingresso a persone non autorizzate, usare sistemi di sicurezza per il controllo accessi.

Impersonation

Descrizione: Fingere di essere una figura di autorità per ottenere fiducia e dati.

Difese: Verificare l'identità prima di fornire informazioni sensibili, implementare protocolli di sicurezza per le comunicazioni interne.

Tecniche di Social Engineering con l'ausilio di Intelligenza Artificiale e Difese

Deepfake

Descrizione: Creazione di video o audio falsi per ingannare la vittima.

Difese: Utilizzare strumenti di rilevamento deepfake, verificare le comunicazioni tramite canali alternativi.

Chatbot AI per Phishing

Descrizione: Chatbot che imitano comunicazioni reali per ottenere informazioni.

Difese: Educare il personale sui rischi dei chatbot, utilizzare autenticazione multi-fattoriale.

Voice Phishing con AI

Descrizione: IA vocali che simulano la voce di persone reali per truffe.

Difese: Implementare soluzioni di riconoscimento vocale avanzate, verificare tramite canali alternativi.

Automazione di Attacchi con IA

Descrizione: IA che automatizzano la raccolta di dati personali.

Difese: Utilizzare sistemi di sicurezza per monitorare e bloccare attività sospette, educare i dipendenti.

Riconoscimento Emotivo con AI

Descrizione: Analisi delle emozioni della vittima per manipolarla.

Difese: Essere consapevoli della manipolazione emotiva, utilizzare tecniche di comunicazione assertiva.

Generazione di Email Personalizzate

Descrizione: Email phishing generate dall'IA basate sullo stile della vittima.

Difese: Implementare soluzioni anti-phishing, educare i dipendenti a riconoscere email sospette.

AI-Driven Social Media Profiling

Descrizione: IA che analizza i profili social per attacchi mirati.

Difese: Limitare le informazioni pubbliche sui social media, utilizzare impostazioni di privacy elevate.

Manipolazione dei Social Bot

Descrizione: IA che gestisce bot per creare relazioni con le vittime.

Difese: Diffidare di interazioni non verificate, educare il personale sui rischi.

Attacchi su Larga Scala con IA

Descrizione: IA usata per lanciare migliaia di attacchi phishing personalizzati.

Difese: Utilizzare soluzioni di sicurezza che blocchino attacchi su larga scala, formare il personale.

Attacchi di Human Augmentation

Descrizione: Assistenti virtuali che aiutano gli attaccanti in tempo reale.

Difese: Verificare sempre le identità e le richieste, utilizzare procedure di sicurezza avanzate.