Social Engineering e Tecniche di Difesa

Introduzione

Il social engineering rappresenta una delle minacce più diffuse e pericolose nell'ambito della sicurezza informatica, poiché non sfrutta vulnerabilità tecniche dei sistemi, ma quelle umane. Gli attaccanti fanno leva su emozioni come fiducia, paura, urgenza o curiosità per indurre le vittime a compiere azioni che compromettono la sicurezza, come rivelare informazioni riservate o concedere accessi non autorizzati. Questo esercizio ha l'obiettivo di comprendere le principali tecniche di social engineering, analizzarne esempi realistici e individuare strategie di difesa efficaci.

Il Social Engineering

Per avviare l'attività è stato formulato un prompt per ChatGPT con l'obiettivo di ottenere una panoramica generale sul social engineering e sulle tecniche più comuni utilizzate dagli attaccanti. Il prompt utilizzato è questo:

"ChatGPT, potresti spiegare cos'è il social engineering e descrivere le tecniche più comuni utilizzate dagli attaccanti, come phishing e tailgating?"

Dall'analisi delle informazioni ottenute emerge che il social engineering è una tecnica di manipolazione psicologica utilizzata per indurre una persona a compiere azioni dannose per la sicurezza. Tra le tecniche più comuni si trova il phishing, che consiste nell'invio di email o messaggi ingannevoli per ottenere credenziali o informazioni sensibili. Un'altra tecnica diffusa è il pretexting, in cui l'attaccante si finge una persona o un'autorità affidabile per ottenere informazioni. Il tailgating invece si verifica quando un individuo non autorizzato riesce ad accedere a un'area protetta seguendo una persona autorizzata senza essere controllato.

Esempi di attacchi di Social Engineering

Gli attacchi di social engineering risultano efficaci perché spesso appaiono credibili e ben costruiti. Un esempio tipico è l'email di phishing che simula una comunicazione ufficiale da parte di una banca o di un'azienda, creando un senso di urgenza che spinge l'utente ad agire rapidamente senza verificare l'autenticità del messaggio. Un altro esempio riguarda le telefonate fraudolente in cui l'attaccante si presenta come un tecnico informatico o un operatore di assistenza chiedendo informazioni riservate per "risolvere un problema". In ambito fisico il tailgating sfrutta la gentilezza o la distrazione delle persone per accedere a edifici o uffici riservati.

Strategie di Difesa contro il Social Engineering

Per contrastare efficacemente gli attacchi di social engineering è fondamentale adottare una combinazione di buone pratiche tecniche e comportamentali. La prima linea di difesa è la consapevolezza degli utenti: riconoscere messaggi sospetti, richieste urgenti o comunicazioni non attese riduce notevolmente il rischio di cadere vittima di un attacco. È importante verificare sempre l'identità del mittente evitando di cliccare su link o allegati provenienti da fonti non sicure.

Un'altra strategia fondamentale è la formazione continua, soprattutto in ambito aziendale, attraverso simulazioni di phishing e corsi di sicurezza informatica. L'uso di strumenti tecnici come filtri antispam, autenticazione a due fattori e politiche di accesso rigorose contribuisce ulteriormente a limitare l'impatto di questi attacchi. Infine, è essenziale adottare una mentalità prudente, ricordando che nessuna organizzazione affidabile richiede informazioni sensibili tramite email o telefono.

Conclusione

Lo svolgimento di questo esercizio ha permesso di comprendere come il social engineering rappresenti una minaccia concreta e spesso sottovalutata, basata principalmente sul fattore umano. Allo stesso tempo, l'utilizzo di ChatGPT per l'analisi dei CVE ha dimostrato come strumenti di intelligenza artificiale possano supportare lo studio e la comprensione delle vulnerabilità informatiche. Combinando consapevolezza, formazione e aggiornamento continuo è possibile migliorare significativamente il livello di sicurezza sia a livello personale che professionale.