Milano, 21 marzo 2024 - Studiare il comportamento delle persone, o meglio delle vittime, con lo scopo di carpire le loro credenziali e utilizzarle per entrare nei sistemi informativi di un'organizzazione. Gli attacchi social engineering continuano a rappresentare un fenomeno allarmante, al punto che Cisco Talos - la più grande organizzazione privata di intelligence al mondo dedicata alla cybersecurity - ha recentemente rilevato che quasi il 40% degli impegni di sicurezza presi in carico dai suoi specialisti ha riguardato proprio l'utilizzo di account validi da parte dei criminali per ottenere l'accesso iniziale a un'organizzazione.

Social engineering: di cosa si tratta?

Il social engineering sfrutta principalmente una tecnica chiamata phishing. In genere, un aggressore si spaccia per qualcuno che la vittima conosce e cerca di trasmettere un senso di urgenza e importanza nelle sue comunicazioni, per incoraggiarlo a cliccare sul suo messaggio.

Ecco le più comuni tecniche di phishing utilizzate per il social engineering:

- **Phishing**: un aggressore invia e-mail o messaggi fraudolenti che sembrano provenire da fonti attendibili per indurre un utente a rivelare informazioni personali.
- **Spear phishing**: una forma di phishing più mirata, in cui la vittima designata è una persona o un'organizzazione specifica. Molto spesso i messaggi fanno riferimento a un collega o a un progetto a cui l'azienda sta lavorando.
- **Whaling**: messaggi che prendono di mira dirigenti di alto livello o persone importanti all'interno di un'azienda.
- **Vishing**: è la versione telefonica del phishing, in cui l'aggressore chiama la vittima e finge di essere un collega o un'organizzazione per chiedere informazioni sensibili.
- **Smishing**: si tratta della versione SMS del phishing, in cui l'aggressore invia messaggi fraudolenti via testo per indurre la vittima a fornire informazioni sensibili.

Come difendersi?

Le minacce informatiche sono in continua evoluzione e sempre più sofisticate, ecco perché è necessario implementare una strategia di sicurezza che garantisca solo accessi affidabili. Le nuove soluzioni permettono di proteggere gli utenti e di impostare blocchi che siano in grado di ostacolare e fermare gli aggressori.

- **Accesso sicuro ai sistemi aziendali**: occorre poter verificare se il dispositivo che si connette è registrato e quindi affidabile.
- **Passwordless**: una password compromessa è ancora il metodo più comune usato da un hacker per entrare nei sistemi aziendali. Oggi è possibile fare a meno delle password e utilizzare al loro posto i dati biometrici, rendendo così inutili gli attacchi di phishing in cui i malintenzionati rubano le credenziali.
- **Valutazione dei rischi in caso di attacco**: è possibile aumentare i criteri per accedere ai sistemi aziendali in un attimo. L'autenticazione di tipo "push" consiste nell'obbligo di inserire manualmente un codice, cosa che un utente abilitato non può fare se non sta effettuando l'accesso.