Guida al Social Engineering

Cos'è il Social Engineering?

Il social engineering è una tecnica utilizzata per manipolare le persone con l'obiettivo di ottenere informazioni sensibili o di convincerle a compiere azioni specifiche, spesso a beneficio di un attaccante. Gli attaccanti sfruttano la fiducia, le emozioni, e l'ignoranza delle vittime per aggirare le misure di sicurezza.

Tecniche più comuni di Social Engineering:

1. Phishing

Il phishing è una delle forme più diffuse di social engineering. Consiste nell'invio di comunicazioni fraudolente, solitamente e-mail o messaggi, che imitano aziende o individui affidabili. L'obiettivo è ingannare la vittima per:

- Ottenere credenziali di accesso (username e password).
- Installare malware sul dispositivo.
- Rubare informazioni finanziarie come numeri di carte di credito.

Esempi comuni di phishing:

- Email fasulle: Un messaggio che sembra provenire dalla banca, chiedendo di verificare le credenziali di accesso.
- Link fraudolenti: Siti web che imitano pagine autentiche per raccogliere dati personali.

2. Tailgating

Il tailgating, o "attacco del portellone", implica l'accesso fisico non autorizzato a un luogo protetto sfruttando la cortesia di qualcuno che apre una porta o cancello. L'attaccante:

- Finge di aver dimenticato il badge o le credenziali.

- Segue un dipendente fidato per accedere a un'area riservata.

Come prevenirlo:

- Non consentire l'accesso a persone sconosciute senza verifica.

- Utilizzare porte con controllo di accesso automatico.

3. Pretexting

In questo caso, l'attaccante crea una storia convincente (un "pretesto") per ottenere informazioni. Può fingere di essere:

- Un tecnico IT che necessita dell'accesso al computer della vittima.

- Un rappresentante di un'organizzazione che richiede dettagli personali.

4. Baiting

Il baiting implica l'uso di un'esca, come una chiavetta USB infetta lasciata in un luogo visibile, per invogliare la vittima a utilizzarla. Quando viene connessa al computer, installa malware o ruba dati.

5. Vishing (Voice Phishing)

Un attacco che utilizza chiamate vocali per ingannare la vittima. L'attaccante potrebbe:

- Fingere di essere un operatore bancario.

- Richiedere dettagli finanziari con urgenza.

Come proteggersi dal Social Engineering:

1. Formazione e sensibilizzazione: Educare le persone a riconoscere i segnali di un attacco.

2. Verifica dell'identità: Non fornire informazioni sensibili senza verificare la legittimità della richiesta.

3. Utilizzo di strumenti di sicurezza: Software anti-phishing e controlli di accesso fisici.

4. Diffidenza verso richieste sospette: Non aprire link o allegati non richiesti.

5. Politiche aziendali: Implementare regole chiare per l'accesso e la protezione dei dati.