Tecniche di Social Engineering e Difese

1. Tecniche di Social Engineering

- Phishing

L'invio di email fraudolente che sembrano provenire da fonti affidabili, spesso con l'obiettivo di rubare informazioni personali come credenziali di accesso o dati bancari.

- Spear Phishing

Una variante più mirata del phishing, in cui l'attaccante personalizza i messaggi per colpire specifici individui o organizzazioni.

- Pretexting

L'attaccante crea uno scenario falso per convincere la vittima a condividere informazioni sensibili. Ad esempio, fingendosi un impiegato dell'azienda.

- Baiting

Offrire un'esca, come un dispositivo USB infetto o un link a un download allettante, per indurre la vittima a compromettere la propria sicurezza.

- Tailgating

Accedere a edifici protetti seguendo da vicino un dipendente autorizzato, spesso fingendo di essere un collega o un visitatore legittimo.

- Vishing

Tecnica che utilizza chiamate vocali o messaggi registrati per ingannare la vittima e ottenere informazioni sensibili o denaro.

Tecniche di Social Engineering e Difese

2. Strategie di Difesa

- Educazione e Consapevolezza

Formare i dipendenti e gli utenti per riconoscere le tecniche di social engineering e agire con prudenza.

- Autenticazione a Due Fattori (2FA)

Implementare il 2FA per aggiungere un livello di sicurezza ai processi di autenticazione.

- Verifica delle Identità

Diffidare di richieste non sollecitate di informazioni sensibili e verificare sempre l'identità del richiedente.

- Protezione dei Dispositivi

Non collegare dispositivi sconosciuti al proprio computer e mantenere aggiornati software e antivirus.

- Politiche di Accesso Fisico

Implementare misure di sicurezza come badge, telecamere e personale addetto al controllo degli accessi.

- Simulazioni di Attacchi

Condurre test di phishing e altre simulazioni per identificare vulnerabilità e migliorare la risposta degli utenti.