S5 L4 Luca Calvigioni

Social engineering e tecniche di difesa

Le tecniche di ingegneria sociale puntano a sfruttare la psicologia umana per ingannare le persone e ottenere informazioni sensibili o accesso a sistemi sicuri. Le tecniche più comuni oggi includono:

Tecniche Comuni di Ingegneria Sociale

1. **Phishing**: Tentativo di ottenere informazioni riservate come password, numeri di carta di credito o credenziali di accesso tramite email, SMS o siti web falsi. Il phishing spesso sfrutta una grafica che imita aziende legittime e richieste urgenti per indurre a cliccare.
2. **Spear Phishing**: Variante più mirata del phishing, rivolta a una persona specifica o a piccoli gruppi. Gli attacchi sono personalizzati e possono fare riferimento a informazioni personali della vittima per sembrare più autentici.
3. **Vishing e Smishing**: Il vishing (voice phishing) si svolge tramite chiamate telefoniche, in cui un truffatore si spaccia per un rappresentante bancario o di un'azienda per convincere la vittima a condividere informazioni. Lo smishing è simile, ma avviene tramite SMS.
4. **Pretexting**: Questa tecnica consiste nel creare un falso pretesto per ottenere informazioni personali. Il truffatore si presenta come una figura autorevole (ad es., un impiegato IT o un funzionario del governo) per convincere le vittime a rivelare dettagli sensibili.

5. **Baiting**: L’uso di "esche" fisiche o digitali, come chiavette USB infette lasciate in luoghi pubblici, o promesse di premi o contenuti gratuiti online. Quando la vittima interagisce con l’esca, può scaricare malware o compromettere i propri dati.
6. **Tailgating e Piggybacking**: Tecniche fisiche in cui un truffatore segue da vicino una persona autorizzata per accedere a una zona riservata (tailgating) o si fa volontariamente far entrare (piggybacking).
7. **Quid Pro Quo**: Qui l’attaccante promette qualcosa in cambio di informazioni o accesso. Un esempio è il truffatore che si presenta come tecnico dell’assistenza e offre di risolvere un problema in cambio di accesso al dispositivo della vittima.

Tecniche di Difesa

1. **Educazione e Formazione**: La prima linea di difesa è comprendere i rischi e sapere come identificare un attacco. Formazioni regolari su phishing e ingegneria sociale aiutano a riconoscere truffe comuni.
2. **Verifica dell’Identità**: Utilizzare sempre metodi di verifica, come richiamare numeri ufficiali, verificare mittenti di email o SMS, e verificare le informazioni su canali affidabili.
3. **Evita di Cliccare su Link e Allegati Non Richiesti**: Non aprire link o allegati di provenienza sconosciuta, anche se sembrano urgenti o legittimi.
4. **Autenticazione a Due Fattori (2FA)**: Questa aggiunge un livello di sicurezza extra, poiché anche in caso di furto delle

credenziali è necessario un secondo fattore per accedere all'account.

5. **Utilizzo di Filtri Anti-Spam e Antivirus**: Filtri anti-spam avanzati e software antivirus aggiornati possono prevenire attacchi di phishing e bloccare malware.
6. **Controllo degli Accessi Fisici**: In uffici o luoghi di lavoro, utilizzare badge, codici di accesso, o biometrici per evitare accessi non autorizzati. Non lasciare dispositivi incustoditi in luoghi pubblici.
7. **Consapevolezza sulle Chiavette USB e i Dispositivi Esterni**: Evitare di inserire chiavette USB o dispositivi trovati in luoghi pubblici, poiché possono contenere malware.

Queste pratiche di difesa, combinate con una buona dose di scetticismo e consapevolezza, possono ridurre notevolmente i rischi di ingegneria sociale.