Guida al Social Engineering

Strategie per Difendersi dagli Attacchi di Social Engineering

1. Formazione e Consapevolezza

La formazione è il primo passo per prevenire gli attacchi di social engineering. Le persone devono essere consapevoli delle tecniche utilizzate dagli attaccanti e dei segnali di avvertimento.

- Organizza corsi di formazione regolari per sensibilizzare dipendenti o utenti.
- Utilizza simulazioni di attacchi (ad esempio, test di phishing) per migliorare la preparazione.

2. Verifica dell'Identità

Prima di fornire informazioni sensibili o accedere a richieste, verifica sempre l'identità del richiedente:

- Richiedi conferme tramite un canale di comunicazione alternativo.
- Evita di fidarti di chiamate o e-mail non sollecitate che richiedono dati personali o aziendali.

3. Implementazione di Politiche di Sicurezza

Definisci regole chiare per la protezione delle informazioni e l'accesso ai dati aziendali:

- Richiedi badge o credenziali per l'accesso fisico ai locali.
- Limita l'accesso ai dati in base al principio del privilegio minimo.

4. Utilizzo di Strumenti di Sicurezza

Adotta strumenti tecnologici per proteggere i tuoi sistemi da potenziali attacchi:

- Installa software antivirus e anti-malware aggiornati.
- Configura filtri anti-phishing per e-mail.

5. Diffidenza verso Comunicazioni Sospette

- Non aprire link o allegati in e-mail sospette.

- Controlla sempre l'URL di un sito web per verificarne l'autenticità.

- Non condividere mai informazioni sensibili tramite e-mail o telefono senza verifica.

6. Controlli di Accesso Fisico

Proteggi le aree riservate con misure di sicurezza fisica:

- Usa serrature elettroniche e telecamere di sorveglianza.

- Evita di permettere l'accesso a persone sconosciute senza verifica.

7. Politiche di Gestione delle Password

- Richiedi l'uso di password complesse e univoche.

- Implementa l'autenticazione a due fattori (2FA).

- Cambia le password regolarmente e non condividerle con altri.

8. Monitoraggio e Risposta agli Incidenti

- Monitora regolarmente i sistemi per individuare comportamenti sospetti.

- Prepara un piano di risposta agli incidenti per gestire eventuali attacchi.