Social engineering

Il Social Engineering è un insieme di tecniche utilizzate dagli attaccanti per manipolare le persone al fine di ottenere informazioni sensibili, accesso a sistemi o beni. Le tecniche più comuni sono:

1. **Phishing:** Gli attaccanti inviano e-mail o messaggi che sembrano provenire da fonti affidabili per indurre le persone a rivelare informazioni personali, come password o numeri di carta di credito. cliccando sul link che ti mandano entrerai in un profilo falso che imita bene quello originale.

2. **Spear Phishing:** A differenza del phishing lo spear phishing è più mirato, vengono raccolte informazioni specifiche per rendere l'attacco ancora più convincente.

3. **Vishing:** Vengono utilizzate delle chiamate telefoniche fingendosi rappresentanti di una banca o di un'agenzia governativa.

4. **Tailgating:** Si verifica quando un attaccante entra fisicamente in un'aera riservata seguendo una persona autorizzata rubando così informazioni.

Per prevenire tutto questo è richiesta una combinazione di consapevolezza, formazione e pratiche di sicurezza, ad sempio:

1. **Formazione e consapevolezza:** Si possono organizzare sessioni di formazioni regolari per i dipendenti su come riconoscere i segnali di attacchi di social engineering, facendo anche simulazioni di phishing per aiutare le persone a riconoscere e saper reagire a tali attacchi.

2. **Verifica delle identità:** Se vengono richieste informazioni sensibili bisogna verificare sempre l'identità della persona e se si riceve un email sospetta, bisogna contattare la persona o l'ente.

3. **Controllo degli accessi:** Utilizza l'autenticazione a due fattori per raggiungere un alto livello di sicurezza degli account.

4. **Attenzione alle comunicazioni:** Controllare sempre l'URL dei siti prima di fornire informazioni sensibili e diffidare di offerte che sembrano troppo belle per essere vere.

5. **Sicurezza fisica:** Implementa sistemi di controllo per le aree sensibili e non collegare USB trovati a computer aziendali.

6. **Utilizzo di software di sicurezza:** Assicurarsi che i dispositivi siano protetti con software antivirus aggiornando e firewall attivi.

Social Engineering

Social engineering is a set of techniques used by attackers to manipulate people in order to obtain sensitive information, access to systems, or assets. The most common techniques are:

- **Phishing:** Attackers send emails or messages that appear to come from reliable sources to induce people to reveal personal information, such as passwords or credit card numbers. By clicking on the link they send, you will enter a fake profile that closely imitates the original.
- **Spear Phishing:** Unlike phishing, spear phishing is more targeted; specific information is gathered to make the attack even more convincing.
- **Vishing:** Phone calls are used, where attackers pose as representatives of a bank or government agency.
- **Tailgating:** This occurs when an attacker physically enters a restricted area by following an authorized person, thus stealing information.

To prevent all of this, a combination of awareness, training, and security practices is required, such as:

- **Training and Awareness:** Regular training sessions can be organized for employees on how to recognize the signs of social engineering attacks, including phishing

simulations to help people recognize and respond to such attacks.

- **Identity Verification:** Always verify the identity of the person requesting sensitive information, and if you receive a suspicious email, contact the person or organization directly.
- **Access Control:** Use two-factor authentication to achieve a high level of account security.
- **Attention to Communications:** Always check the URL of websites before providing sensitive information and be wary of offers that seem too good to be true.
- **Physical Security:** Implement control systems for sensitive areas and do not connect found USB devices to company computers.
- **Use of Security Software**: Ensure that devices are protected with updated antivirus software and active firewalls.