Social Engineering

Definition:
Unter Social Engineering versteht man die Beeinflussung von Personen, um bestimmte Verhaltensweisen hervorzurufen. Das Ziel ist es dem Opfer vertrauliche Information zu entlocken oder auch ihn/sie zum Kauf eines Produktes zu bewegen. Des weiteren täuschen Social Engineers Identitäten vor und spionieren das persönliche Umfeld des Opfers aus.
Wenn Social Engineering zum Eindringen in ein fremdes Computersystem dient, wird es auch als Social Hacking bezeichnet.

Formen:
Die zwei bekanntesten Formen des Social Engineering sind **Phishing** und **Dumpster Diving**.

- **Phishing**
  Dem Opfer wird eine vertraute E-mail geschickt. Der Inhalt der E-mail kann zum Beispiel sein, dass es bei der Bank es Opfers technische Probleme gab, und nun die Daten neu anfordern muss.
- **Dumpster Diving**
  Hierbei wird der Müll des Opfers durchwühlt und nach Hinweisen und Anhaltspunkten über das soziale Umfeld gesucht. Mit den gesammelten Daten, kann man das Vertrauen des Opfers gewinnen.

Abwehr:
Sich gegen Social Engineers zu schützen ist nicht so einfach, da sie im Grunde die positiven menschlichen Eigenschaften ausnutzen.
Dennoch sollten folgende Punkte unbedingt beachtet werden:

- Unklare Identität des Absenders einer E-Mail nicht trauen.
- Beim Antworten einer E-Mail keine persönlichen oder finanziellen Daten preisgeben.
- Unbekannten Anrufer keine Daten verraten.
- Keine Links aus E-Mails verwenden, die persönliche Daten als Eingabe verlangen.