Social Engineering

Beim Social Engineering (auf Deutsch etwa „soziale Manipulation“) versuchen Kriminelle durch gezielte Beeinflussung, Menschen zu einem bestimmten Verhalten zu bewegen – etwa der Herausgabe von vertraulichen Informationen wie z. B. Passwörtern.

Vorgehensweise

Beim Social Engineering spionieren Kriminelle das Umfeld des Opfers aus oder versuchen sich durch geschickte Manipulation oder Täuschung sensible Informationen von Unternehmen, aber auch Privatleuten zu erschleichen. Häufig finden die Angriffe telefonisch statt. Dabei werden von den Kriminellen oft entweder die Hilfsbereitschaft und das Vertrauen der Opfer oder aber der Respekt vor Vorgesetzten ausgenutzt. Ist der Anrufer vom Opfer einmal als vertrauenswürdig eingestuft, kann er oftmals sehr gezielt sensible Informationen abfragen.

Typische Szenarien

Typische Szenarien bei Social Engineering sind zum Beispiel:

Vermeintliche IT-Mitarbeiter müssen angeblich einen Systemfehler beheben und fragen dazu bei Angestellten Passwörter ab.

Angebliche Wartungs- oder Entstörungsdienste melden sich, weil sie für ihre Arbeit bestimmte technische Einstellungen abfragen müssen – oder bitten die Beschäftigten selbst Änderungen am System durchzuführen.

Externe Anrufer erkundigen sich nach einem Kollegen, der nicht erreichbar ist. Durch die Info, dass dieser zwei Wochen Urlaub hat, wissen die Angreifer, dass sein E-Mail-Account und ggf. sein Büro in dieser Zeit unbeobachtet sind.

Das vermeintliche Sekretariat aus der Führungsebene braucht dringend Passwörter oder andere sensible Informationen.

Ein Anrufer fragt auf den ersten Blick unwichtig erscheinende Informationen ab. Kombiniert können diese Daten dann eine relevante Information ergeben.

Siehe auch:
Cybergrooming
Datenschutz

Zurück