



Social Engineering

Informationsbeschaffung
durch soziale Manipulation



Wirtschaft & Wissenschaft.
Zukunftssicher.

Verfassungsschutzverbund des Bundes und der Länder

41%

BETROFFENE UNTERNEHMEN
laut Bitkom Research 2021

DARUM GEHT ES.

Social Engineering nutzt gezielt individuelle Persönlichkeitsmerkmale aus, um Menschen zu manipulieren. So gelangen Angreifer an Daten, mit denen sie sich Zugriffsmöglichkeiten auf wertvolle Informationen verschaffen.

SO LÄUFT ES AB.

1. Informationssammlung über Personen, Unternehmen, Strukturen – zumeist über offene Quellen wie z. B. Webseiten, soziale Netzwerke.
2. Nutzung der Informationen zum Beziehungsaufbau – Kontakt per Telefon, E-Mail, über soziale Netzwerke oder persönlich.
3. Ausnutzung menschlicher Eigenschaften – Hilfsbereitschaft, Angst, Vertrauen, Respekt, Unaufmerksamkeit, Neid, Mitleid.
4. Zugriff auf gewünschte Informationen – mittels Internet, Schadsoftware, virtueller bzw. physischer Zugänge oder durch menschliche Informationsträger.

SO SCHÜTZEN SIE SICH.

- offene Fehlerkultur etablieren
- Hilfestellungen bei der Nutzung sozialer Medien
- klare Prozesse und Verantwortlichkeiten definieren
- fortlaufende Sensibilisierungen der Beschäftigten für verschiedene Angriffssituationen
- Umsicht bei der Weitergabe von unternehmensinternen Informationen

**IM ZWEIFELSFALL GILT:
SICHERHEIT GEHT VOR.**

**IHR DIREKTER KONTAKT
ZUM WIRTSCHAFTSSCHUTZ:**