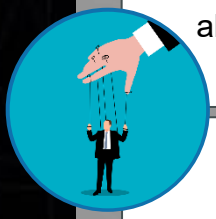
NEWSLETTER
Social Engineering

Was ist Social Engineering?

Bei Social Engineering wird der Mensch als Schwachstelle betrachtet. Noch so gute technische Maßnahmen nützt nichts, wenn der Mensch, der mit diesem System arbeitet, gedankenlos agiert. Kriminelle nutzen den „Faktor Mensch“ als vermeintlich schwächstes Glied der Sicherheitskette aus, um an sensible Informationen zu kommen.



Was sind gängige Betrugsmaschen?

Die Täter nutzen Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität aus, um die Betroffenen geschickt zu manipulieren. Sie sollen vertrauliche Informationen preisgeben, Sicherheitsfunktionen aushebeln, Überweisungen tätigen oder Schadsoftware installieren. Dies erreichen die Täter durch:

- Vortäuschung einer persönlichen Beziehung
- Falsche Gewinnversprechen
- Täter gibt sich als Techniker von Unternehmen aus (z. B. PayPal, Bank)
- Täter gibt sich als Systemadministrator aus

Als Medium kommen sowohl Phishing-Mails, Telefonanrufe, SMS oder auch Nachrichten über die Social Media zum Einsatz

Die Täter sind sehr geübt in der Manipulation ihrer Opfer. Die Opfer, die auf die Täuschung hereinfällt, handeln oft in gutem Glauben, das Richtige zu tun

Wie kann man sich gegen Social Engineering schützen?

- Verantwortungsvoller Umgang mit sozialen Netzwerken
  Persönliche Informationen können von Kriminellen gesammelt und für Täuschungsversuche missbraucht werden. Geben Sie hier keine vertraulichen Informationen über sich oder Ihren Arbeitgeber preis.
- Passwörter, Zugangsdaten oder Kontoinformationen niemals weitergeben
  Banken und seriöse Firmen fordern Ihre Kunden nie per Mail oder Telefon zur Preisgabe von vertraulichen Informationen auf.
- Misstrauen Sie E-Mails von unbekannten Absendern
  Vergewissern Sie sich ggf. durch einen Anruf beim Absender oder der Absenderin, dass es sich um eine legitime E-Mail handelt.

Noch Fragen?
Wenden Sie sich gerne an Ihre Ansprechpartner für die Informationssicherheit: isb@hs-kehl.de