

CSBW

CYBER
SICHERHEITS
AGENTUR
BADEN-WÜRTTEMBERG

Social Engineering

Cyber-Kriminelle nutzen das sogenannte Social Engineering, um Personen zwischenmenschlich zu beeinflussen, sensible Daten preiszugeben, Schutzmaßnahmen zu umgehen oder Schadprogramme auf ihrem Rechner zu installieren.¹

Die nachfolgenden Informationen helfen Ihnen, sich erfolgreich vor Angriffen zu schützen.



Eine Schwachstelle, für die es keine technischen Sicherheitsmaßnahmen gibt:

- ▶ Cyber-Kriminelle nutzen den „**Faktor Mensch**“ als vermeintlich schwächstes Glied in der Sicherheitskette aus.¹
- ▶ Sie bedienen sich typisch **menschlicher Eigenschaften** wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität.
- ▶ Klassische Merkmale sind das **Vortäuschen einer falschen Identität** und das **Vertuschen der tatsächlichen, schädlichen Absichten**:

Beispielsweise gibt sich eine Person am Telefon als Systemadministrator aus, um vertrauliche Informationen und Zugangsdaten (z.B. Passwort) für eine angebliche Behebung eines Sicherheitsproblems zu erfragen.¹

- ▶ Personen, die auf solche Täuschungen hereinfallen, handeln immer in dem **guten Glauben**, das Richtige zu tun.

So schützen Sie sich vor Social Engineering:

► Verantwortungsvoller Umgang

Gehen Sie verantwortungsvoll mit Ihren persönlichen Informationen und sensiblen Daten Ihres Arbeitsumfeldes um. Achten Sie besonders in sozialen Netzwerken darauf, welche Informationen Sie preisgeben, da diese im Rahmen von Social Engineering-Angriffen gegen Sie verwendet werden könnten.

► Bewusstsein schaffen

Seien Sie aufmerksam, welche potenziell sensiblen Informationen Sie über Ihre Arbeitsstelle und Ihre Arbeit teilen.

► Keine Auskunft

Teilen Sie Passwörter, Zugangsdaten und Kontoinformationen niemals per Telefon oder E-Mail mit.

► Besondere Vorsicht

Seien Sie bei E-Mails von unbekanntem Adressen besonders vorsichtig und misstrauisch. Es könnte sich um einen Phishing-Angriff handeln.

► Gesundes Misstrauen

Misstrauen Sie Personen (auch Führungskräften), die Sie durch Druck zu einer sicherheitsriskanten Handlung bewegen möchten.

► Durch schnelles Handeln können mögliche Schäden verhindert werden

Wenn Sie befürchten, Opfer von Social Engineering geworden zu sein, informieren Sie schnellstmöglich Ihre Vorgesetzten und die beauftragte Person für Informationssicherheit (ISB).

Formen des Social Engineering:

► Phishing

Informationen dazu im CSBW-Factsheet „Phishing-E-Mails“.

► CEO-Fraud

Betrügerinnen und Betrüger geben sich als Führungskraft aus und versuchen Mitarbeitende so zu manipulieren, dass diese beispielsweise Überweisungen hoher Geldbeträge oder Zugang zu sicherheitsrelevanten Bereichen gestatten.

► Privates Umfeld

Enkelkind-Trick oder Vortäuschung eines Lotteriegewinns. Bitte wenden Sie sich bei Verdacht an eine Polizeidienststelle.

Quellen:

¹ https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html