CSBW
CYBER SICHERHEITS AGENTUR
BADEN-WÜRTTEMBERG

So schützen Sie sich vor manipulativen Angriffen!

CSBW-Factsheet: Cybersecurity-Wissen kompakt

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** der Kriminellen.
  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.

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.

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.
- **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 unbekannten 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.

Quelle:

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

Weitere Factsheets und Informationen unter: www.cybersicherheit-bw.de

CSBW – Abteilung 1: Prävention – Stand 04.2023
Kontakt: schulungen@cybersicherheit.bwl.de