Cybersicherheitsagentur Baden-Württemberg
(CSBW)

CSBW CYBER SICHERHEITS AGENTUR BADEN-WÜRTTEMBERG

Barrierefreie Version
CSBW-Factsheet: Cybersecurity-Wissen kompakt

Zum Thema: SOCIAL ENGINEERING

So schützen Sie sich vor manipulativen Angriffen!

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:

1. Cyber-Kriminelle nutzen den **„Faktor Mensch“** als vermeintlich schwächstes Glied in der Sicherheitskette aus.[1]
2. Sie bedienen sich typisch **menschlicher Eigenschaften** wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität.
3. 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]
4. Personen, die auf solche Täuschungen hereinfallen, handeln immer in **dem guten Glauben**, das Richtige zu tun.

So schützen Sie sich vor Social Engineering:

1. **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.
2. **Bewusstsein schaffen**
   Seien Sie aufmerksam, welche potenziell sensiblen Informationen Sie über Ihre Arbeitsstelle und Ihre Arbeit teilen.
3. **Keine Auskunft**
   Teilen Sie Passwörter, Zugangsdaten und Kontoinformationen niemals per Telefon oder E-Mail mit.
4. **Besondere Vorsicht**
   Seien Sie bei E-Mails von unbekannten Adressen besonders vorsichtig und misstrauisch. Es könnte sich um einen Phishing-Angriff handeln.

5. **Gesundes Misstrauen**
   Misstrauen Sie Personen (auch Führungskräften), die Sie durch Druck zu einer sicherheitsriskanten Handlung bewegen möchten.
6. **Durch schnelles Handeln können mögliche Schäden verhindert werden.**
   Wenn Sie befürchten, Opfer von Social Engineering geworden zu sein, informieren Sie schnellstmöglich Ihre Vorgesetzten.

Formen des Social Engineering:

1. **Phishing**
   Informationen dazu im CSBW-Factsheet „Phishing-E-Mails“.
2. **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.
3. **Privates Umfeld**
   Enkelkind-Trick oder Vortäuschung eines Lotteriegewinns. Bitte wenden Sie sich bei Verdacht an eine Polizeidienststelle.

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