Info Blatt

Informationsblätter zum Wirtschaftsschutz

Schutz vor Social Engineering

Hinweise für Beschäftigte

Social Engineering ist eine der bedrohlichsten Formen des Informationsdiebstahls, da sie direkt am Menschen ansetzt. Angreifende bedienen sich dabei unterschiedlichster Methoden, um ihr Ziel zu erreichen. Sie als Beschäftigte können sich davor schützen: durch umfassendes Wissen und gesundes Misstrauen.

Dabei können auch die Sicherheitsbehörden hinzugezogen werden. Der Verfassungsschutz ist für die Abwehr von Spionage und Sabotage durch ausländische Nachrichtendienste zuständig und steht als vertraulicher Ansprechpartner zur Verfügung.

Das sollten Sie wissen.

- Beim Social Engineering nutzen angreifende Personen gezielt **menschliche Eigenschaften** aus, um Sie **zu manipulieren**, wie z. B.
  - Hilfsbereitschaft
  - Angst
  - Neugier
  - Vertrauen
  - Respekt vor Autorität

Ziel ist es, **Sie dazu zu verleiten**, vertrauliche Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln oder Schadsoftware zu installieren.

Social Engineering kennt viele Angriffswege.
Das grundlegende Vorgehen ist dabei immer ähnlich.

Informationssammlung *über Personen und Unternehmen*

Beziehungsaufbau und Manipulation *(E-Mail, Telefon, Social-Media, persönlich)*

Erhalt der *gewünschten* ***Informationen***

JEDER IST GEFÄHRDET

→ *Nicht nur Personen mit Zugang zu sensiblen Informationen können Opfer von Social Engineering werden. Auch scheinbar harmlose Informationen können für Angreifende interessant sein und für weiterführende Angriffe genutzt werden.*

So können Sie sich schützen.

Social-Media/Business-Kanäle

- Social-Engineering-Profis nutzen veröffentlichte persönliche und berufliche Daten für eine spätere Kontaktaufnahme, z. B. per E-Mail oder Telefon. Es besteht auch die Gefahr, dass Sie über Fakeprofile kontaktiert werden.

- **Überprüfen Sie regelmäßig Ihre Datenschutz-Einstellungen.**
- **Posten Sie keine Firmendaten und befolgen Sie vorhandene Social Media Guidelines.**
- **Seien Sie wachsam bei Kontaktaufnahmen und evtl. ungewöhnlichen beruflichen Angeboten.**

Beispiel: *Auf einem Karriereportal wird ein Biotechnologe von einer vermeintlichen Kollegin kontaktiert. Der Spezialist fühlt sich schnell geschmeichelt und teilt seine wissenschaftliche Expertise. Dabei gibt er auch sensible interne Informationen weiter.*

So können Sie sich schützen.

E-Mail

- Hierbei handelt es sich zumeist um den Versuch, Sie mittels E-Mails dazu zu bewegen, Anhänge zu öffnen oder Passwörter preiszugeben. Angreifende Personen nutzen dazu häufig vorher recherchierte Informationen, um den Inhalt der E-Mail auf Sie zuzuschneiden.

- **Geben Sie niemals Passwörter oder Zugangsdaten an.**
- **Führen Sie den 3-Sekunden-Sicherheitscheck durch: Ist der Absender bekannt? Ist der Betreff sinnvoll? Wird ein Anhang von diesem Absender erwartet?**
- **Lassen Sie sich nicht unter Druck setzen und sichern Sie sich ggf. bei der absendenden Stelle durch Rückfrage ab.**

Beispiel: *Ein Softwareingenieur erhält über den Social-Business-Account eines mutmaßlichen Konkurrenzunternehmens den Hinweis auf eine interessante Position. Unter einem Vorwand wird ihm später die Stellenausschreibung über seine berufliche E-Mail-Adresse zugesandt. Das Dokument enthält jedoch eine Schadsoftware.*

Telefon

- Angriffe erfolgen auch telefonisch. Ziel ist es, sich Informationen wie z. B. Passwörter zu erschleichen oder Zugang zu Computern zu erhalten. Mittels vorher ausgekundschafteter Informationen wird Vertrauen oder Autorität aufgebaut.

- **Zeigen Sie stets ein gewisses Maß an Misstrauen bei unerwarteten Anrufen.**
- **Prüfen Sie z. B. über Nachfragen die Identität der anrufenden Person.**
- **Unterbrechen Sie ggf. unter einem Vorwand das Telefonat und holen Sie eine Zweitmeinung ein.**

Beispiel: *Eine Mitarbeiterin wird durch einen vorgeblichen Systemadministratoren wegen einer angeblichen Behebung eines Softwarefehlers angerufen. Da der Anrufer anscheinend mit dem betriebsinternen Softwareprogramm vertraut ist, teilt ihm die Mitarbeiterin ihre Zugangsdaten mit.*

Weitere Sicherheitstipps

- **Verwenden Sie niemals USB-Sticks zweifelhafter Herkunft in Verbindung mit betrieblicher oder privater Technik und seien Sie wachsam bei kostenlosen Downloadangeboten.**
- **Sprechen Sie in der Öffentlichkeit nicht über betriebsinterne Angelegenheiten und nutzen Sie zudem einen Sichtschutz für Ihren Laptop.**

→ *Nutzen Sie ggf. die Möglichkeit, sich an Ihre sicherheitsbeauftragte Person oder die Sicherheitsbehörden zu wenden.*

Wirtschaft & Wissenschaft. Zukunftssicher.
Verfassungsschutzverbund des Bundes und der Länder

Das Bundesamt für Verfassungsschutz und die 16 Landesbehörden für Verfassungsschutz bilden gemeinsam den Verfassungsschutzverbund. Auch im Bereich des präventiven Wirtschaftsschutzes arbeitet dieser eng zusammen. Auf diese Weise entsteht ein starkes Netzwerk bis zu Ihnen vor Ort. Eine Übersicht über die Ansprechbarkeiten in den Landesbehörden finden Sie unter ***www.verfassungsschutz.de****.*

initiative wirtschaftsschutz
Gemeinsam. Werte. Schützen.

Die Initiative Wirtschaftsschutz ist ein Zusammenschluss von BfV, BKA, BND und BSI. Auf der Informationsplattform ***www.wirtschaftsschutz.info*** *stellen sie zusammen mit verschiedenen Partnerverbänden ihre Expertise im Bereich Wirtschaftsschutz zur Verfügung. Dazu gehört das Thema Cyberkriminalität genauso wie Wirtschafts- und Wissenschaftsspionage oder das Thema IT-Sicherheit.*

Ihr direkter Kontakt zum Wirtschaftsschutz