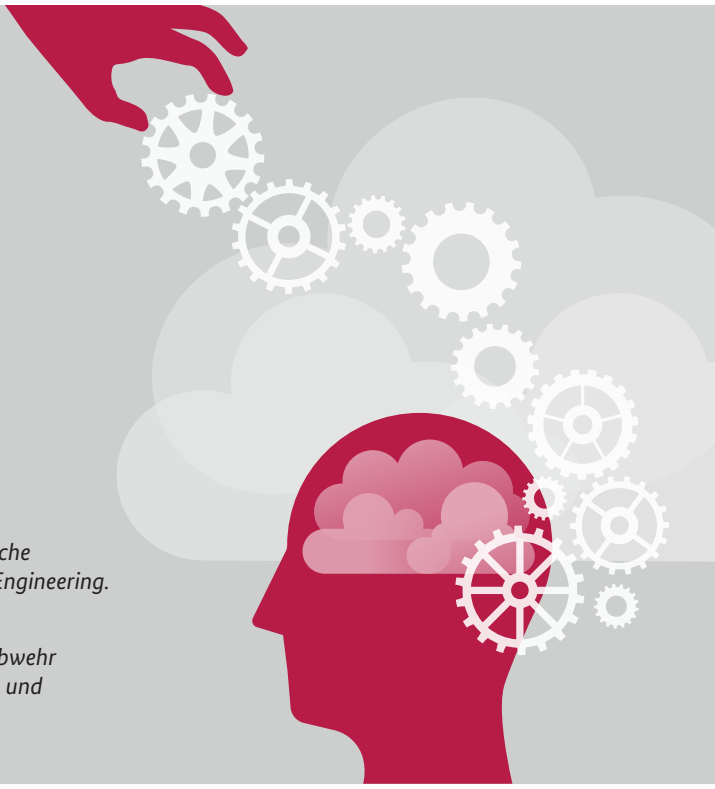
Info Blatt

Informationsblätter zum Wirtschaftsschutz

Schutz vor Social Engineering

Hinweise für Leitungsebene und Sicherheitsverantwortliche



Die deutsche Wirtschaft und Wissenschaft, aber auch Politik und Verwaltung wurden in der Vergangenheit Ziel von Spionage und Sabotage durch ausländische Nachrichtendienste. Eine der gängigen Angriffsmethoden ist dabei das Social Engineering.

Mögliche Gefährdungen lassen sich jedoch minimieren. 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.

1 Was ist Social Engineering?

- Beim Social Engineering nutzen angreifende Personen gezielt **individuelle Persönlichkeitsmerkmale** aus, um Menschen **zu manipulieren**, wie z. B.
  - Hilfsbereitschaft
  - Angst
  - Neugier
  - Vertrauen
  - Respekt vor Autorität
- Ziel ist es, die angegriffene Person **dazu zu verleiten**, vertrauliche Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln oder Schadsoftware zu installieren.

SOCIAL ENGINEERING KENNT VIELE ANGRIFFSWEGE.

- Direkte **telefonische** Kontaktaufnahme, um z. B. an weiterführende Informationen zu gelangen
- **Persönliche Treffen**, z. B. bei Messen oder – vermeintlich zufällig – auf einer Dienstreise
- Ansprache über **Social-Media/Business-Kanäle**
- **Computerbasierte Angriffe** mit personalisierten Inhalten mittels ***(Spear-)Phishing-E-Mails***
- **Auslegen von Ködern**, wie z. B. USB-Sticks

2 So läuft ein Social-Engineering-Angriff ab.

Ein Social-Engineering-Angriff kann in **verschiedene Phasen** unterteilt werden.

1	2	3	4
Informationssammlung	***Beziehungsaufbau***	***Manipulation***	***Zugriff auf Informationen***
Organisation und Aufbau des Unternehmens, eingesetzte Hard- und Software, Namen und Position von Beschäftigten	*Kontakt per Telefon, E-Mail, über soziale Netzwerke oder persönlich*	*Ausnutzung menschlicher Eigenschaften – Hilfsbereitschaft, Angst, Vertrauen, Respekt, Unaufmerksamkeit, Neid, Mitleid*	*Möglichst unbemerkt mittels Internet, Schadsoftware, virtueller bzw. physischer Zugänge oder durch menschliche Informationstragende*
Leitfrage: ***Welche Unternehmensinformationen sind öffentlich zugänglich?***	*Leitfrage:* ***Welches sind die möglichen Angriffswege und wie lassen sich diese schützen?***	*Leitfrage:* ***Wie können Beschäftigte im Umgang mit Manipulationsversuchen gestärkt werden?***	*Leitfrage:* ***Wie lassen sich Unternehmensdaten – auch im Ernstfall – am besten schützen?***

Alle Phasen bieten die Möglichkeit, unternehmensspezifische Schutzmaßnahmen abzuleiten.

3 So schützen Sie sich.

Generell gilt:
Ermitteln Sie zunächst durch eine möglichst vollständige Risikoanalyse die besonders schützenswerten Güter („Key Assets"), mögliche Angreifende und potentielle Angriffswege. Leiten Sie aus der Risikoanalyse entsprechende Schutzmaßnahmen ab.

1 Informationssammlung

- Geben Sie Ihren Beschäftigten **Hilfestellungen bei der Nutzung sozialer Medien**. Regeln Sie insbesondere den Umgang mit organisationsbezogenen Daten.
- Gehen Sie umsichtig bei der **Weitergabe von unternehmensinternen Informationen** vor.
- Verzichten Sie auf Ihrer **Internetseite** auf die Nennung von Namen, Darstellung der Unternehmensstruktur oder Durchwahlnummern. Nutzen Sie möglichst **generische E-Mail-Adressen** für die Kontaktaufnahme, bspw. info@unternehmen.de.
- Veröffentlichen Sie in **Stellenausschreibungen** nur wirklich notwendige Informationen. Diese können von Angreifern genutzt werden, um **bei Kontaktaufnahmen vertrauenswürdiger** zu erscheinen.
- Lassen Sie Ihre **Liegenschaften** bei Anbietern von Satellitenanwendungen **unkenntlich machen**.
- Stellen Sie in Abhängigkeit vom Schutzbedarf der Informationen eine **Abfallrichtlinie** auf. Damit verhindern Sie, dass Angreifende über das sogenannte ***Dumpster Diving*** an sensible Daten gelangen.

DEEPFAKES – SOCIAL ENGINEERING 2.0

Bei Deepfakes werden durch Künstliche Intelligenz manipulierte Ton- oder Videodateien geschaffen. Dies bietet Angreifende zukünftig ganz neue Möglichkeiten, Menschen zu manipulieren (Telefon- bzw. Videoanrufe). Gleichzeitig wird es mit zunehmender Rechenleistung immer schwerer, gefälschtes Material zu identifizieren.

Dumpster Diving
Dabei durchsuchen angreifende Personen den Müll eines Unternehmens systematisch nach Informationen wie z. B. Kennwörter oder Zugangsdaten. Aber auch Telefonlisten, Organigramme oder Hinweise auf genutzte Computerprogramme können für Social-Engineering-Angriffe genutzt werden.

2 Beziehungsaufbau

- Identifizieren Sie mögliche **Wege und Endpunkte einer Kontaktaufnahme** und entwickeln Sie passende Schutzmechanismen.
- **E-Mails sind ein kritischer Angriffsweg.** Daher sollten die Beschäftigten in der Lage sein, ***(Spear-)Phishing-Mails*** zu erkennen und damit umzugehen.
- Bei Informationsanfragen oder unerwarteten Kontaktaufnahmen sollte unbedingt die **Identität der anfragenden Person überprüft** werden – auch bei Kontakten per E-Mail oder Telefon.
- Richten Sie eine **IT-Sicherheitsstelle** ein, die für Rückfragen der Beschäftigten, z. B. zu potentiellen Phishing-E-Mails, zur Verfügung steht.

(Spear-)Phishing
Unter dem Begriff Phishing versteht man Versuche, mittels gefälschter Webseiten, E-Mails oder Kurznachrichten an persönliche Daten von Internetnutzerinnen und -nutzern, insbesondere Login-Informationen, zu gelangen.
Spear-Phishing ist dagegen auf bestimmte Personen, Unternehmen oder Organisationen ausgerichtet. Dabei kommen vorher gewonnene spezifische Informationen zum Einsatz.

ZWANZIG MINUTEN

Viele unternehmensbezogene Informationen lassen sich frei im Internet recherchieren: Auf Social-Business-Kanälen, in Stellenausschreibungen oder auf der Unternehmenswebseite finden Widersacher Informationen, die sie für Social-Engineering-Angriffe nutzen können.
So benötigte die Teilnehmerin eines Hackingwettbewerbs lediglich 20 Minuten, bis ein Angestellter des Zielunternehmens ihr Auskünfte sowohl über die IT-Ausstattung und die installierte Software des Unternehmens gab, als auch zwei ihm benannte Internetadressen aufrief. Die Angreiferin hatte sich als IT-Kollegin ausgegeben und konnte auf Grundlage der vorher recherchierten Informationen über das Unternehmen das Vertrauen der Person erlangen.

3 So schützen Sie sich.

3 Manipulation

- Etablieren Sie in Ihrem Unternehmen eine **offene Fehlerkultur**.
- Setzen Sie ggf. **Wachpersonal** ein und sichern Sie **Zugänge zu sensiblen Bereichen** zusätzlich ab.
- **Sensibilisieren Sie die Beschäftigten** fortlaufend für die verschiedenen Angriffssituationen (Verhalten bei Telefonanrufen, Verwendung von Speichermedien, Umgang mit E-Mail-Anhängen etc.). Ermöglichen Sie eine **praxisnahes Erleben** durch Fallstudien und Rollenspiele.

Der Mensch ist der erste Ansatzpunkt für mehr Sicherheit.

BEISPIEL

Der Angestellte eines mittelständischen Unternehmens fand auf dem Parkplatz einen Schlüsselbund, an dem sich auch ein USB-Stick befand. Da der Angestellte sich Informationen zur besitzenden Person erhoffte, verband er den Stick mit dem Bürocomputer. Mit fatalen Folgen, denn der USB-Stick wurde von den Angreifenden mit einer Schadsoftware versehen und absichtlich auf dem Firmenparkplatz hinterlassen.

4 Zugriff auf Informationen

- **Klassifizieren Sie Unternehmensdaten** (z. B. öffentlich, intern, vertraulich, geheim) und reglementieren Sie über ein **Berechtigungskonzept** die Zugriffe auf Daten.
- Geben Sie Ihren Beschäftigten **klare Anweisungen** und stellen Sie Ihnen **Ablaufprozeduren zur Verfügung**, wie im Ernstfall vorzugehen ist.
- Halten Sie eingesetzte **Software immer auf dem aktuellsten Stand**, auch auf den im Homeoffice genutzten Endgeräten.
- Neben der Verwendung von **Antivirenprogrammen** und **Firewalls** sollten Sie auch den Einsatz von **Content-Filtern**, **Anti-Spam** und **Anti-Phishing-Programmen**, sogenannten **Intrusion Detection Systems** (IDS) und anderer Sicherheitsstandards prüfen.
- Blockieren Sie **USB- und CD-Ports** bzw. untersagen Sie die Verwendung fremder oder privater Datenträger.
- Erhöhen Sie, wenn möglich, auch die **physischen Sicherheitsvorkehrungen**: Personenkontrollen, Überwachungskameras, Alarmanlagen, Sicherheitstürschlösser etc.
- Stellen Sie Richtlinien für den **Umgang mit Besuchern** auf (Besucherausweise, Begleitpersonen etc.).
- Stellen Sie ggf. durch technische Maßnahmen sicher, dass alle Mitarbeiterinnen und Mitarbeiter **sichere Passwörter** verwenden.
- Entwickeln Sie ein **Notfallmanagement** – so können Sie im Ernstfall den Geschäftsbetrieb aufrechterhalten.

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