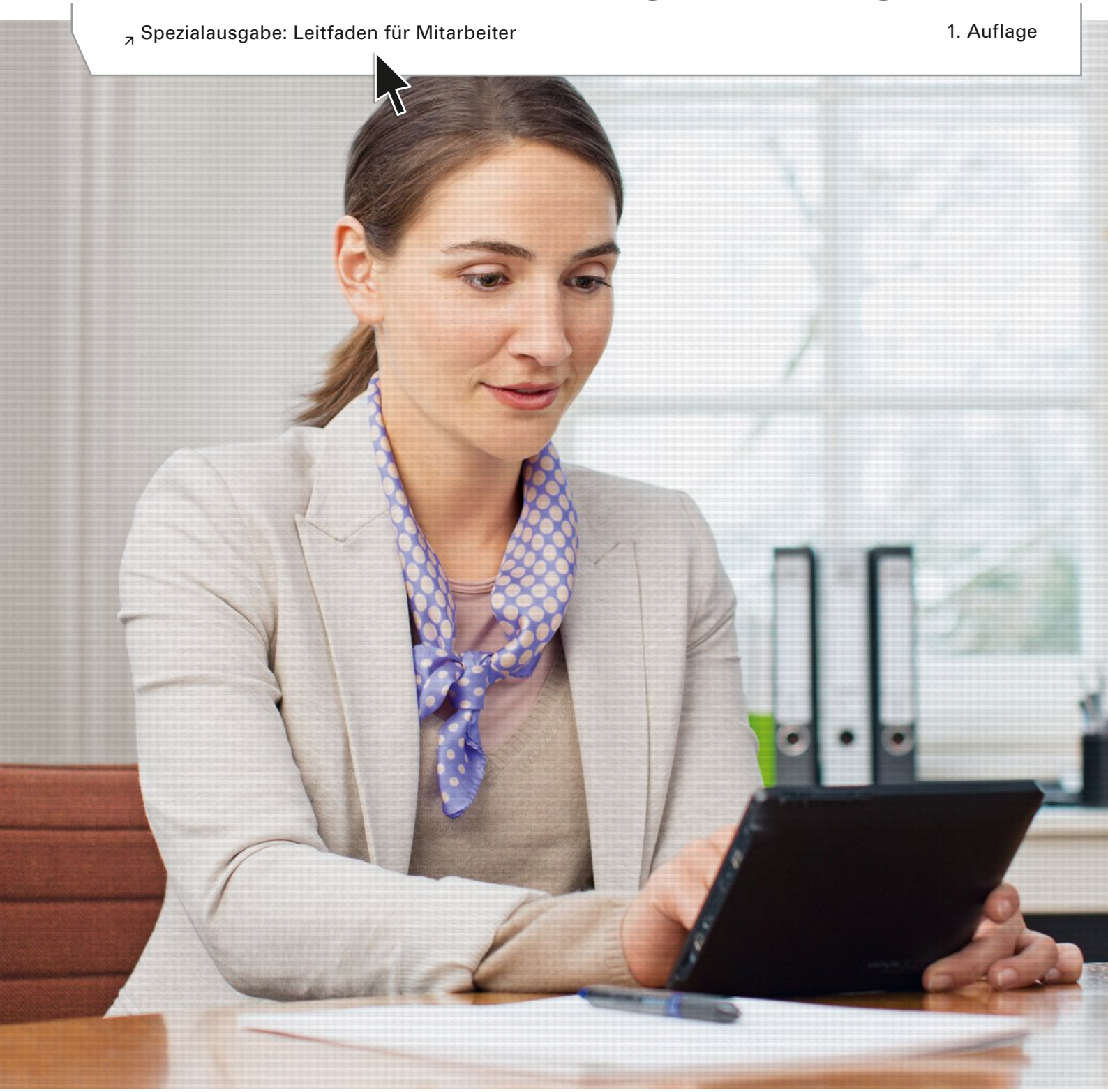
Verhaltensregeln zum Thema „Social Engineering“

↗ Spezialausgabe: Leitfaden für Mitarbeiter

1. Auflage



↗ Eine Informationsbroschüre von DATEV und Deutschland sicher im Netz e.V.

Schirmherrschaft

Bundesministerium des Innern

Deutschland sicher im Netz

Vorwort

Berichte über erfolgreiche Cyberattacken auf Unternehmen gehören inzwischen zum Alltag. Dabei wird immer häufiger der „Faktor Mensch" als „Sicherheitslücke" ausgenutzt – mit sogenannten Social-Engineering-Angriffen. Laut einer aktuellen Studie des Digitalverbands Bitkom (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.) wurden in den vergangenen zwei Jahren 51 % aller Unternehmen in Deutschland Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl. Der dadurch entstehende Schaden beläuft sich auf rund 51 Milliarden Euro pro Jahr. Fast ein Fünftel (19 %) der befragten Unternehmen hatten dabei auch Social-Engineering-Angriffe registriert.[1] Das würde in Deutschland also hochgerechnet mehr als 60.000 Unternehmen betreffen – plus solche Firmen, bei denen entsprechende Versuche unentdeckt bleiben.

Unternehmen und Privatpersonen bieten viele Angriffsmöglichkeiten für Social Engineers

Der Begriff „Social Engineering" bezeichnet in der IT-Sicherheit Angriffsmethoden, bei denen die Kriminellen durch die Manipulation von Personen an sensible Informationen von Unternehmen oder Privatpersonen zu gelangen versuchen. Das Risiko solcher Angriffe steigt heute auch durch die zunehmende Nutzung von sozialen Netzwerken und die vielfältigen Möglichkeiten, sich im Internet mit Bekannten und Unbekannten auszutauschen. Die Bereitschaft von Mitarbeitern, über Social Media Informationen über sich und über etablierte Prozesse in ihrem Unternehmen preiszugeben, bietet Angreifern eine breitere Basis zur gezielten Vorbereitung von Social-Engineering-Attacken.

Ein umfassendes Wissen und gesundes Misstrauen sind die beste Prävention gegen Social-Engineering-Angriffe

Kein IT-Sicherheitssystem der Welt kann Daten schützen, die von ihren rechtmäßigen Nutzern freiwillig herausgegeben werden. Es ist daher ungemein wichtig, dass die Mitarbeiter selbst sich grundlegendes Wissen über Social-Engineering-Methoden aneignen, ein gesundes Misstrauen gegenüber Dritten entwickeln, das Gefahrenpotenzial verschiedener Risikosituationen einschätzen können und sich ein sicherheitsbewusstes Verhalten in ihrem Alltag antrainieren.

Um diesen Lernprozess zu fördern, haben DATEV und die Initiative „Deutschland sicher im Netz e. V." die vorliegenden „Verhaltensregeln zum Thema Social Engineering" entwickelt. Als Fortsetzung zu unserem Mitarbeiter-Leitfaden „Verhaltensregeln zur Informationssicherheit" können Unternehmer diese Spezialausgabe gezielt einsetzen, um ihre Mitarbeiter für die Gefahren des Social Engineering zu sensibilisieren und mit wirksamen Schutzstrategien auszustatten.

[1] www.bitkom.org, Bitkom: „Digitale Angriffe auf jedes zweite Unternehmen". Befragt wurden im Januar und Februar 2014 insgesamt 1.074 Unternehmen ab 10 Mitarbeitern

Anhand einiger besonders gefährdeter Lebens- und Arbeitsbereiche macht der Leitfaden Unternehmer und ihre Mitarbeiter auf konkrete Risiken durch Social-Engineering-Attacken im Arbeitsalltag aufmerksam, gibt einen kompakten und allgemein verständlichen Überblick und motiviert zu einem sicherheitsbewussten Umgang mit entsprechenden Situationen. Klare Verhaltensregeln am Ende jedes Kapitels sowie Hinweise zu weiterführenden Informationen unterstützen bei der Umsetzung des Gelernten. Zusätzlich enthält der Leitfaden einen Testfragebogen, mit dem die Mitarbeiter und Mitarbeiterinnen selbst überprüfen können, wie anfällig sie noch für Social Engineering sind, sowie einen Erinnerungs-Kalender mit integrierter Karte, der Ihnen dabei helfen soll, in ihrem beruflichen Alltag stets achtsam zu bleiben.

Wir wünschen Ihnen eine angenehme Lektüre und hoffen, dass unsere Publikation Ihnen hilft, Ihr Unternehmen besser vor Cyber-Attacken zu schützen!

Dr. Henning Gulden
Leiter
DATEV-Gesamtsicherheitsgremium

Dr. Michael Littger
Geschäftsführer
Deutschland sicher im Netz e. V.

Verhaltensregeln zum Thema „Social Engineering“

Spezialausgabe: Leitfaden für Mitarbeiter

Social Engineering wird von vielen Sicherheitsbeauftragten als die gefährlichste Form des Informationsdiebstahls angesehen. Im Bereich IT-Sicherheit gilt der Mensch selbst als der größte Risikofaktor. Denn Menschen sind manipulierbar – nicht weil sie dumm oder schwach wären, sondern weil sie von klein auf gelernt haben, sich kooperativ zu verhalten. Die Basis jeder Kooperation aber ist Vertrauen und deshalb haben viele von uns es verlernt, auch einmal zu misstrauen, wenn es angebracht ist. Außerdem ist es vielen Menschen unangenehm, anderen einen dringenden Wunsch abzuschlagen, und nicht wenige haben auch Angst, sich gegenüber scheinbaren Autoritätspersonen zu behaupten. Kriminelle oder Spione nutzen solche ganz normalen menschlichen Eigenschaften aus, um ihre Ziele zu erreichen.

Das gilt übrigens nicht nur für Unternehmensdaten: Auch als Privatperson sind Sie gefährdet, denn wichtige persönliche Informationen, z. B. Zugangsdaten für das Online-Banking, können ebenfalls gestohlen werden, wenn Sie einem Social-Engineering-Angriff zum Opfer fallen.

Gesundes Misstrauen muss gelernt werden

Jeder Mensch mit Zugang zu sensiblen Informationen ist potenziell eine Gefahr für die Sicherheit. Deswegen reichen software- und hardwareseitige Abwehrvorkehrungen bei Weitem nicht aus, um Informationsdiebstahl vollständig zu verhindern. Unternehmen sind darauf angewiesen, dass ihre Mitarbeiter geschäftliche Informationen sorgsam behandeln und sich ihrer Bedeutung für das Unternehmen bewusst sind. Die Mitarbeiter müssen zudem wissen, welche konkreten Gefahren es „da draußen“ gibt, wie man Manipulationsversuche erkennt und wie man Informationsdiebstahl verhindern kann. Und selbst dieses Wissen reicht längst noch nicht aus: Weil das Social Engineering sich tief verwurzelter menschlicher Verhaltensmuster und Motivationen bedient, muss seine Abwehr den Mitarbeitern in Fleisch und Blut übergehen.

Ziel dieses Leitfadens

Das bedeutet im Klartext: Vertrauen unter Kollegen ist sehr wichtig, aber spezielle Situationen erfordern auch ein gesundes (also nicht paranoides, sondern rationales) Misstrauen – nicht nur gegen unbekannte Anrufer, sondern mitunter selbst gegenüber Menschen, die Sie z. B. in der Pause treffen.

Informationssicherheit muss gelebt werden

Informationssicherheit ist nicht allein Sache der IT-Abteilung, sondern durchdringt jeden Bereich des Unternehmens. Nötig ist eine Verankerung von Risikobewusstsein, Schutzmaßnahmen und geeigneten Regeln in der gelebten Unternehmenskultur. Dieser Leitfaden soll Ihnen dabei helfen, den ersten Schritt zu tun: Er erläutert besondere Risikosituationen und formuliert konkrete Verhaltensregeln und Tipps für die Praxis, um Manipulationen zu vereiteln. Diese Regeln müssen aber – das ist der zweite Schritt – durch klare Vorgaben im Unternehmen unterstützt werden. Denn nur wenn z. B. Rückfragen zur Identitätsprüfung als normale Routine gelten und nicht als Ausdruck von Unfreundlichkeit, wird jeder sie mit gutem Gewissen ausführen.

Dieser Leitfaden hilft Mitarbeitern, sich effektiv für Social-Engineering-Angriffe zu sensibilisieren.

Entsprechend kann der vorliegende Leitfaden zur Mitarbeiterschulung verwendet, aber auch als Grundlage für die Weiterentwicklung des Sicherheitskonzepts herangezogen werden. Darüber hinaus können Sie sich mit dem Test am Ende des Leitfadens selbst auf Ihre Social Engineering Awareness testen und Sie erhalten einen Erinnerungs-Kalender, der Sie täglich an das A und O der Social-Engineering-Abwehr erinnern soll:

Gesundes Misstrauen lohnt sich! Jeden Tag!

1 Was ist Social Engineering?

„Soziale Ingenieure"? Was soll das denn heißen? Tatsächlich wird der Begriff „Social Engineering" üblicherweise nicht übersetzt, sondern auch im Deutschen als Fachbegriff verwendet. Der Begriff stammt ursprünglich aus den Sozialwissenschaften und meint dort die Beeinflussung von Einstellungen und Verhalten mit sozialen Mitteln und für (meist positive) soziale Zwecke. Dahinter steht die Annahme, Menschen und die sozialen Strukturen, in denen sie sich bewegen (etwa am Arbeitsplatz), funktionierten ähnlich wie Maschinen nach vorhersehbaren Regeln, die von Wünschen, Ängsten und etablierten Verhaltensmustern bestimmt werden.

Heute wird „Social Engineering" fast immer auf spezifische Bedrohungen der Informationssicherheit bezogen, die sich ebenfalls psychologischer Manipulationen – nämlich Täuschung und Betrug – bedienen, um menschliches Verhalten zu beeinflussen und so an sensible Informationen von Unternehmen oder Privatpersonen zu gelangen. Im Gegensatz zum „normalen" (technischen) Hacking nutzen die Angreifer also nicht die Schwachstellen eines Computersystems aus, um an geheime Informationen zu gelangen, sondern die Schwachstellen des Menschen. In Hacking-Kreisen wird daher auch von „Social Hacking" gesprochen.[2]

Die Vergabe von komplexen Passwörtern hilft, Ihre Daten zu schützen.

Ziele der Angreifer

Der Verwendungszweck der mittels Social Engineering beschafften geschützten Informationen (z. B. geschäftskritische, vertrauliche und andere interne Informationen eines Unternehmens, Login-Daten, Transaktionsnummern für Online-Banking, Kontodaten, Kreditkarten-PINs, persönliche Informationen etc.) kann variieren, z. B.:

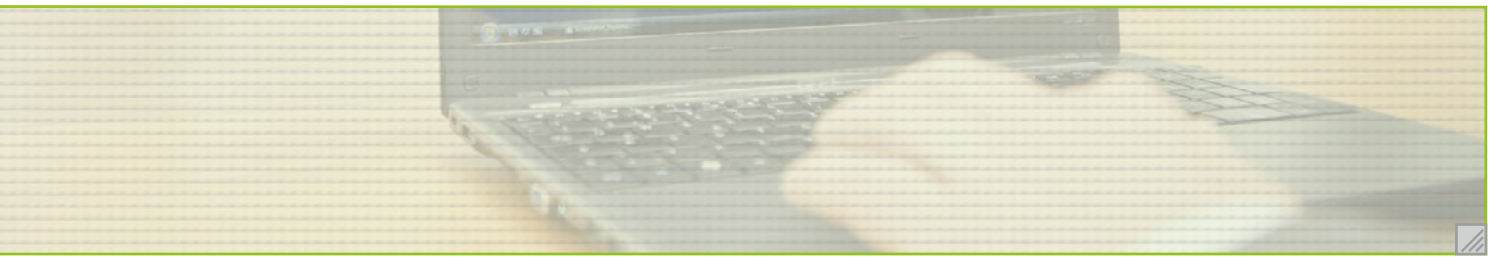
- **Industriespionage**, um Wettbewerbsvorteile zu sichern
- **Identitätsdiebstahl**, um etwa Dienstleistungen oder Waren kostenfrei zu erhalten, die Reputation des Opfers zu schädigen, Kredite aufzunehmen etc.
- **Image- oder Rufschädigung** eines Unternehmens oder einer Person
- **Erpressung** durch die beschaffenen Informationen
- **Zugriff auf weitere Datensysteme**

Ein Hauptziel solcher Angriffe aber sind Passwörter: Allein im vergangenen Jahr wurden mehr als 150 Mio. Accounts durch Passwort-Diebstahl gehackt.[3]

Allgemeine Vorgehensweise bei Angriffen

Auch Sie sind wahrscheinlich schon mehr als einmal mit Social Engineering in Berührung gekommen! Denn fast jeder Internet-Nutzer hat in seinem Leben schon sogenannte Phishing-E-Mails erhalten, die ihn auffordern, Daten – z. B. Kontodaten – in ein Formular einzugeben, oft auf einer überzeugend gestalteten Webseite, die aussieht wie die einer großen Bank oder eines populären Online-

[2] www.computec.ch, siehe z. B. die Kategorieseite „Social Hacking" des Security-Onlinearchivs
[3] www.breachalarm.com/



Dienstes. Andere Spam-Mails versuchen etwa den Empfänger dazu zu bringen, eine Schadsoftware auszuführen: Das Bundeszentralamt für Steuern warnte im Mai 2015 vor E-Mails, die in seinem Namen und dem Betreff „Rückerstattung/refund“ eine Schadsoftware verbreitete.

Eine gefälschte Absenderadresse, die mehr oder weniger überzeugende Gestaltung der Mail oder der Zielwebseite – all das soll den Empfänger täuschen und sein Vertrauen erwecken. Denn alle Social-Engineering-Methoden haben gemeinsam, dass sie versuchen, anstelle eines normalen Verhaltensmusters – unserer Skepsis gegenüber möglichen Täuschungsversuchen – ein anderes, ebenso normales Reaktionsmuster hervorzurufen, welches etwa durch Hilfsbereitschaft, Autoritätsgläubigkeit, Mitleid, Gier oder auch Gedankenlosigkeit ausgelöst wird (mehr dazu im nächsten Kapitel). Um das zu erreichen, schmeicheln sich die Angreifer in der Regel anonym oder unter einer falschen Identität beim Opfer ein, erbitten seine Hilfe, betonen die Dringlichkeit ihres Anliegens und setzen das Opfer unter Druck, etwa indem sie drohen, seinen Vorgesetzten einzuschalten. Technische Mittel (wie beim Phishing) spielen dagegen beim Social Engineering nur eine untergeordnete Rolle.

Social-Engineering-Angreifer machen sich insbesondere die Hilfsbereitschaft der Opfer zunutze.

Häufig sind solche Angriffe zudem nur die Vorstufe von weiteren Social-Engineering- oder Hacking-Attacken. Denn in Abhängigkeit vom Schutzniveau ihrer Angriffsziele bedienen sich Social Engineers häufig sehr komplexer Angriffsmuster mit mehreren Phasen, ausgearbeiteten Täuschungsszenarien und langer Vorbereitungszeit, in der Informationen gesammelt und Beziehungen aufgebaut werden. Solche Angriffe können somit jeden Mitarbeiter im Unternehmen treffen und auch noch so unwichtig erscheinende Informationen können dem Angreifer bereits behilflich sein.

Behalten Sie deshalb eines im Hinterkopf: Jeder kann zum Ziel eines Social-Engineering-Angriffes werden – sowohl beruflich wie auch privat! Und jeder Mensch ist auch angreifbar, denn die größte Sicherheitslücke ist heute der Mensch. Mit diesem Thema wird sich das folgende Kapitel beschäftigen. Auf einige besonders gefährdete Lebens- und Arbeitsbereiche wird dagegen in den Kapiteln 3 bis 7 ausführlich eingegangen.

Jeder kann zum Ziel eines Social-Engineering-Angriffs werden und ist angreifbar!

Weiterführende Informationen und Links

- Allgemeine und aktuelle Informationen rund um das Thema Informationssicherheit im Unternehmen bietet der IT-Sicherheitsblog von „Deutschland sicher im Netz“ **www.dsin-blog.de**
- Anregungen zur Weiterbildung in IT-Sicherheitsthemen erhalten Sie unter **www.it-informationssicherheit.de**
- Einen empfehlenswerten Artikel zum Thema „Social Engineering“ des Bundesamts für Sicherheit in der Informationstechnik (BSI) finden Sie unter folgendem Pfad: **www.bsi.bund.de > Themen > IT-Grundschutz > IT-Grundschutz-Kataloge > G5 Vorsätzliche Handlungen > G 5.42 Social Engineering**
- Mehr Informationen rund um „Social Engineering“ hält das IKT-Sicherheitsportal der österreichischen Regierung bereit. Pfad: **www.onlinesicherheit.gv.at > Mitarbeiter/innen > Computer- und Datensicherheit > Social Engineering**

2 Hauptrisiko „Faktor Mensch“

Bleiben Sie achtsam!

Die internen Netzwerke vieler Unternehmen verfügen mittlerweile über sehr sichere Schutzsysteme (z. B. Firewalls, Virenschutz, Verschlüsselung) und sind selbst für erfahrene Hacker schwer zugänglich. Deshalb ist heute der Mensch Risikofaktor Nr. 1, da er oftmals leichter zu „hacken“ ist als das System. So hält der ehemalige Hacker und heutige Sicherheitsexperte Kevin Mitnick, dem es über Jahre hinweg gelang, in einige der am besten gesicherten Computersysteme der USA einzudringen, Social Engineering für die bei Weitem effektivste und schnellste Methode, um an Passwörter zu gelangen. Aus seiner Sicht ist Social Engineering rein technischen Ansätzen weit überlegen.

Welche menschlichen Eigenschaften und Schwächen werden genutzt?

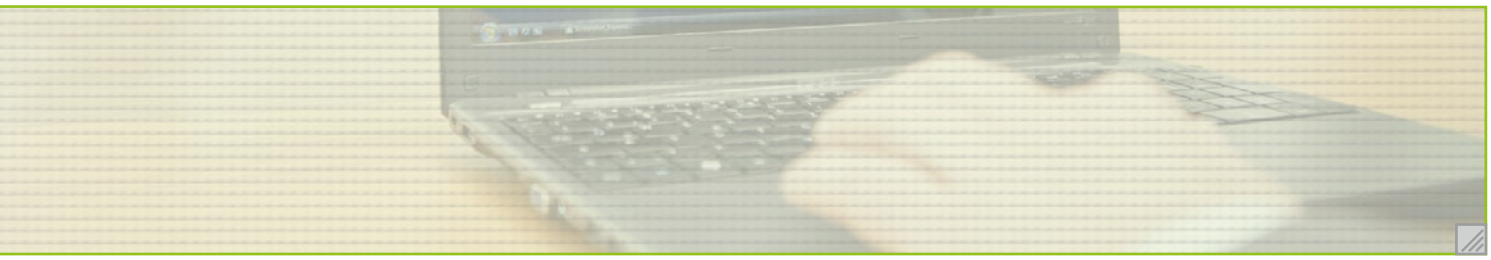
Wie bereits erwähnt, nutzt ein Social Engineer menschliche Wünsche, Ängste und verbreitete Verhaltensmuster aus, um seine Opfer zu manipulieren.

Wünsche:
Eines der wichtigsten Bedürfnisse, das Social Engineers ausnutzen, ist der Wunsch, sich kooperativ und hilfsbereit zu verhalten. Die Methode ist noch wirksamer, wenn sie mit Mitleid gekoppelt wird: So geben sich Angreifer zum Beispiel als gestresste Kollegen aus, die unter Druck stehen. Aber auch eigennützige Wünsche können zur Angriffsfläche werden: Zum Beispiel nutzt der sogenannte Vorschussbetrug die Gier des Opfers, das in Vorleistung gehen soll, um später einen hohen Gewinn zu realisieren (vgl. Schneeballsysteme). Ausgenutzt werden also zum Beispiel die folgenden Wünsche:

- in Notsituationen unbürokratisch zu helfen,
- auf Hilfe mit Gegenhilfe zu reagieren,
- störungsfreie Abläufe zu gewährleisten,
- materiellen Gewinn zu erzielen,
- sich vor der Führungskraft auszuzeichnen,
- der/dem attraktiven Kollegin/Kollegen zu gefallen.

Ängste:
Unser Bedürfnis, Schaden zu vermeiden, richtet sich oft auf die gleichen Inhalte wie die oben genannten Wünsche. Wir möchten nicht negativ auffallen, als unkooperativ erscheinen und womöglich dadurch dem Unternehmen Nachteile verursachen. Angreifer nutzen etwa die Angst:

- Arbeitsabläufe zu behindern und damit Schaden anzurichten,
- vor der Führungskraft schlecht dazustehen,
- einen wichtigen Kunden (durch Unwissenheit) nicht angemessen zu behandeln und vielleicht zu verlieren,
- unseren Mitmenschen nicht zu gefallen.



Automatische Reaktionen und Charaktereigenschaften:
Die meisten Entscheidungen werden nicht ausschließlich bewusst und nach reiflicher Überlegung getroffen, sondern gesteuert durch erfahrungsbedingte Automatismen und Reaktionsmuster sowie durch Charaktereigenschaften. Zum Beispiel vertrauen wir im Zweifel eher bekannten Personen als unbekannten und wir orientieren uns an Autoritäten und Fachleuten – beides sind normalerweise sinnvolle Faustregeln, die uns aber im Fall von Social Engineering angreifbar machen. Die Gefahr, dann falsche Entscheidungen zu treffen, wächst noch, wenn wir besonders unsicher sind und/oder unter Druck stehen. So nutzen Social Engineers häufig Unsicherheiten ihrer Opfer (z. B. technische Unwissenheit, fehlende Vertrautheit mit den Unternehmensabläufen) aus: Sie überzeugen durch selbstbewusstes Auftreten und Fachjargon, drohen vielleicht damit, die Führungskraft einzuschalten, verunsichern das Opfer und erhöhen so die Wahrscheinlichkeit, dass es dem Angreifer hilft. Häufig ausgenutzte Reaktionsmuster und Eigenschaften sind:

- Vertrauen in bekannte Personen
- Vertrauen in unbekannte Personen mit gemeinsamen Bekannten
- Vertrauen in Autoritäten (Autoritätsgläubigkeit)
- die Neigung zu schnellen Entscheidungen
- unüberlegtes Handeln unter Druck und Unsicherheit
- Gutgläubigkeit und Hilfsbereitschaft
- Gier und Eitelkeit
- Angst, Respekt und Scham
- Nachlässigkeit in der täglichen Routine

Wer ist besonders gefährdet?

Prinzipiell kann jeder Mitarbeiter Ziel eines Social-Engineering-Angriffs werden. Dennoch gibt es bevorzugte Zielgruppen für Social Engineers – zum einen Mitarbeiter, bei denen man besonders wertvolle Informationen vermutet, zum anderen solche, die als besonders anfällig für Angriffe erscheinen. Gefährdet sind insbesondere:

- in technischen Fragen unsichere Mitarbeiter und Unternehmer,
- unerfahrene Personen, die mit den Verhältnissen im Unternehmen nicht sehr vertraut sind (neue Mitarbeiter, Auszubildende, Studenten etc.),
- Mitarbeiter mit häufigem Kontakt zu unternehmensfremden Personen, z. B. im Vertrieb oder Service,
- AssistentInnen von Top-Managern,
- Manager,
- generell alle Mitarbeiter, die nicht für das Thema Social Engineering sensibilisiert wurden.

Bitte beachten Sie:
Es kann jeden treffen!

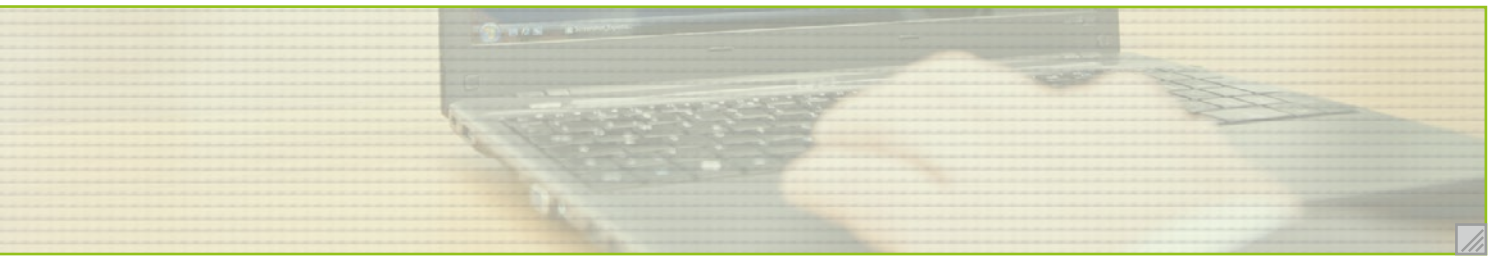
Verbreitet ist die Annahme, Manager und Führungskräfte seien vor Social-Engineering-Angriffen geschützt, weil sie in solchen Themen geschult sind und die Angreifer nicht das Risiko eingehen wollen, ertappt zu werden. Auf der anderen Seite sind aber gerade diese Personen aufgrund ihres Wissens wertvolle Social-Engineering-Ziele und oft auch ideale Opfer: Denn egal wie versiert ein Mitarbeiter, eine Führungskraft oder ein Manager in technischen Fragen ist, so bietet er doch Angriffsflächen, wenn er sich seiner Schwächen in Bezug auf Social Engineering nicht bewusst ist.

Aber auch Mitarbeiter ohne direkten Zugang zu unternehmenskritischen Informationen können zum Ziel solcher Angriffe werden, weil diese oft mehrstufig aufgebaut sind und im ersten Schritt nur Informationen über andere Mitarbeiter gesammelt werden sollen.

Sensibilisierung und Loyalität

Ebenso wie die Social-Engineering-Angriffe selbst müssen auch Abwehrmaßnahmen dagegen beim „Faktor Mensch" ansetzen. Das A und O ist die Sensibilisierung, z. B. durch Schulungen und andere Awareness-Maßnahmen. Prävention geht aber noch weiter: Sie beginnt schon bei der Arbeitsatmosphäre im Unternehmen. Fühlt sich ein Mitarbeiter im Unternehmen unwohl und vermisst er Anerkennung durch Vorgesetzte und Kollegen, dann ist er empfänglicher für Lob und Schmeicheleien von außen. Unternehmen sollten gezielt die Loyalität ihrer Mitarbeiter fördern, um das Risiko zu minimieren, dass diese aus Ärger oder Resignation sensible Daten weitergeben, um dem Unternehmen zu schaden. Wichtig ist auch die Vermeidung von Druck und Angst.

Denn zum einen sind, wie oben erläutert, verunsicherte Mitarbeiter anfälliger für Angriffe. Zum anderen aber wird dadurch die Aufklärung von Vorfällen erschwert: Wenn ein Mitarbeiter bei einem Social-Engineering-Angriff unwissentlich sensible Daten weitergegeben und dies erst im Nachhinein bemerkt hat, wird er sich aus Angst vor einer Abmahnung oder fristlosen Kündigung scheuen, den Vorfall zu melden. Deshalb müssen die Mitarbeiter stets als Opfer und nicht als Mittäter angesehen werden. Nur wenn das Unternehmen zeitnah von Sicherheitsvorfällen erfährt, können vielleicht noch rechtzeitig größere Schäden vermieden und zukünftige Angriffe abgewehrt werden.



3 Risiko Social Network

Bleiben Sie achtsam!

Michaela, 32 Jahre alt, ist seit Kurzem in einem Social Network aktiv und begeistert von den vielen Möglichkeiten, mit Bekannten und Unbekannten in Kontakt zu treten, persönliche Informationen, Bilder und Videos mit ihren Freunden zu teilen und immer auf dem Laufenden zu bleiben. Auch die Anregungen, die sie von Freunden mit ähnlichen Interessen erhält, weiß sie zu schätzen.

Ist Michaela sehr interessiert an einem geposteten Beitrag, klickt sie auch manchmal auf weiterführende Links im Artikel oder auf Links zu empfohlenen (mit „Gefällt mir" markierten) Beiträgen. Natürlich weiß sie, dass man im Internet Vorsicht walten lassen muss, doch fühlt sie sich auf der sicheren Seite, da sie nur Inhalte seriöser und bekannter Seiten verfolgt.

Wo liegen mögliche Gefahren in Michaelas Verhalten?

Soziale Netzwerke bieten viele einfache Möglichkeiten, um mit Fremden in Kontakt zu treten.

„Social Networks", zu Deutsch „soziale Netzwerke", sind in: Fast anderthalb Milliarden Menschen weltweit (1,49 Mrd.) nutzen beispielsweise Facebook, fast 970 Millionen davon täglich.[4] In Deutschland hat Facebook geschätzte 28 Millionen Mitglieder (Stand 2014)[5], von denen 18 Prozent ihr Netzwerk gar für „unverzichtbar" halten.[6] Soziale Netzwerke geben ihren Mitgliedern die Möglichkeit, auf einfache Weise mit anderen Menschen zu kommunizieren und virtuell zu interagieren. Gleichzeitig aber stellen sie ideale Plattformen für Social-Engineering-Angriffe dar, denn:

- a) Soziale Netzwerke sind unerschöpfliche Informationsquellen für Social Engineers.
  Die hohe Dichte an persönlichen Daten und ihr hoher Vernetzungsgrad nehmen dem Social Engineer die größte Arbeit ab: das Nachfragen und Recherchieren. Mit diesen Informationen über eine Person können Angreifer leicht auf Passwörter schließen, die Identität einer Person für eigene Zwecke nutzen oder die Kontakte der Person ausspähen. Viele Menschen geben in ihrem Profil an, für welches Unternehmen sie arbeiten. Findet der Angreifer unter den Freunden bzw. Kontakten einer Person weitere Kollegen, kann er diese im Namen der Person kontaktieren und so vielleicht an vertrauliche Informationen gelangen.

- b) Die Nutzer sozialer Netzwerke kennen viele ihrer Freunde gar nicht.
  Grund Nr. 1: Nutzer populärer Netzwerke haben meist Hunderte Kontakte oder Freunde, von denen sie viele noch nie gesehen haben. Der durchschnittliche Facebook-Nutzer hat einer Studie von 2013[7] zufolge 342 Freunde. Grund Nr. 2: Soziale Netzwerke verlangen meist keine Identifizierung zur Profilerstellung. Jeder kann sich als eine x-beliebige Person ausgeben. So können sich Social Engineers als vermeintliche Bekannte das Vertrauen ihrer Opfer erschleichen, sich als besonders attraktiv dar-

[4] investor.fb.com, offizielle Facebook-Zahlen für das 2. Quartal 2015
[5] www.statista.de, Anzahl der aktiven Nutzer von Facebook in Deutschland von Januar 2010 bis Mai 2014
[6] www.hubert-burda-media.de, Studie von TÜV und Statista im Auftrag von Hubert Burda Media, Oktober 2014
[7] blog.stephenwolfram.com, Data Science of the Facebook World, Stephen Wolfram 2013

stellen oder auch Profile bzw. Seiten von Prominenten oder seriösen Unternehmen (z. B. auch Zeitungen, Organisationen, Parteien) fälschen. Anfang 2010 gelang es einer attraktiven Dame namens Robin Sage, über soziale Netzwerke zahlreiche Militärs, Industrielle und Politiker zu kontaktieren und ihnen im Laufe der Zeit vertrauliche Informationen zu entlocken. Die angebliche Cyberthreat-Analystin stellte sich später als Kunstfigur in einem Experiment des US-IT-Experten Thomas Ryan heraus.[8]

↗ c) Social Engineers können hier direkt mit ihren Opfern in Kontakt treten.
Dabei wird der Social Engineer sein Opfer meist nicht sofort direkt ansprechen, sondern sich langsam in der Freundesliste etablieren. Schickt er seinem Opfer dann eine Kontaktanfrage, werden bereits einige gemeinsame Kontakte angezeigt und lassen das Opfer glauben, dass es sich um eine reale und im Freundeskreis bekannte Person handelt.

↗ d) Manche Nutzer klicken ohne nachzudenken auf von Freunden empfohlene Links.
Ein solcher Link kann dann auf speziell präparierte Seiten weiterleiten, die z. B. gefälschte Informationen enthalten können, um eine Täuschung zu unterstützen, die Eingabe persönlicher Daten fordern, um vermeintlich interessante Inhalte ansehen zu können, oder aber Malware verbreiten.

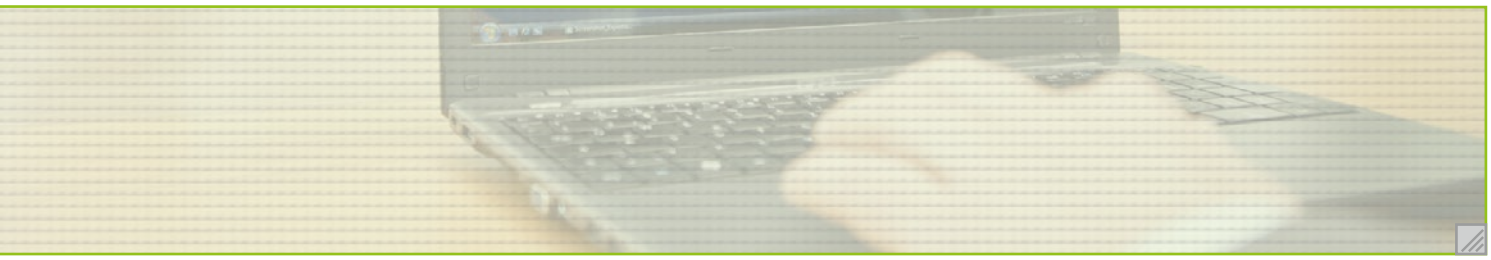
Verbote fruchten nicht

Soziale Netzwerke können nicht verboten werden. Deshalb ist die Sensibilisierung besonders wichtig!

Soziale Netzwerke sind heutzutage aus dem privaten wie beruflichen Alltag nicht mehr wegzudenken. Seiten wie Facebook, Twitter, Instagram oder Xing sind fester Bestandteil moderner Kommunikation. Es ist damit fast unmöglich, sie im Unternehmen zu verbieten. Nicht zuletzt bieten diese Plattformen für Unternehmen auch große Chancen, etwa als Vermarktungskanäle und zur Erhöhung des Bekanntheitsgrades, und auch die Mitarbeiter können dort durchaus als Botschafter des Unternehmens fungieren. Anstelle von Verboten empfiehlt es sich daher, Verhaltensrichtlinien („Social Media Guidelines") einzuführen und Aufklärung zu betreiben. Ausführliche Informationen und Beispiele finden Sie am Ende dieses Kapitels.

↗ **Bitte beachten Sie:**
Ihr Profil und andere Daten in sozialen Netzwerken bieten Social Engineers vielfältige Angriffsmöglichkeiten!

[8] www.sueddeutsche.de, Trickreicher Hackerangriff – Ein kurzes, heißes Leben; Camilo Jiménez 2010



Risiken

1. Ihre im sozialen Netzwerk veröffentlichten Informationen können weitergegeben werden oder gegen Sie verwendet werden.
2. Ein unbemerktes Sammeln Ihrer Daten könnte der Vorbereitung eines Social-Engineering-Angriffs dienen.
3. Durch die Nutzung sozialer Netzwerke erhöht sich das Risiko, Viren oder Schadprogramme zu erhalten. Dies ist vor allem am Arbeitsplatz zu bedenken.

Verhaltensregeln

1. Akzeptieren Sie keine Freundschaftsanfrage ohne Prüfung. Erkundigen Sie sich über Ihnen unbekannte Personen genau (z. B. im Internet, bei gemeinsamen Kontakten). Widersprüchliche Aussagen im Profil (Wohnort, Kontakte, Firma etc.) sind verdächtig.
2. Überprüfen Sie regelmäßig Ihre Privatsphäre-Einstellungen und checken Sie, für wen die Inhalte Ihres Profils sichtbar sind. Seien Sie vorsichtig bei der Auswahl der Informationen, die Sie auf Ihrem Profil preisgeben.
3. Sensible Daten (Kontodaten, firmeninterne Informationen) sind **niemals** über soziale Netzwerke weiterzugeben.

Weiterführende Informationen und Links

- Auf der DATEV-Webseite finden Sie als Beispiel die Social Media Guidelines von DATEV. Pfad: **www.datev.de > Über DATEV > DATEV im Web > Social Media Guidelines**
- Gefahren durch Social Networks für Unternehmen und Mitarbeiter werden hier kurz dargestellt: **www.it-sicherheit-in-der-wirtschaft.de > Themen > Soziale Netzwerke**
- Weitere Möglichkeiten des Missbrauchs sozialer Netzwerke beschreibt das BSI. Pfad: **www.bsi.bund.de > Themen > IT-Grundschutz-Kataloge > Inhalt > Gefährdungskataloge > G 5 Vorsätzliche Handlungen > G 5.158 Missbrauch sozialer Netzwerke**
- Informationen von DSiN: **www.sicher-im-netz.de > Für Verbraucher > E-Mails und Soziale Netzwerke**
- Tipps für Unternehmen des Bitkom zum Thema Social Media Guidelines können Sie hier downloaden: **www.bitkom.org > Publikationen > Leitfaden > Social Media Guidelines – Tipps für Unternehmen** (Suchfunktion vorhanden)
- Einen Artikel zum Thema Social Media im Unternehmen finden Sie unter **www.dsin-blog.de > Themen > News & Trends > „Social Media im Unternehmen – Fluch oder Segen?“**
- Dem technischen Umgang mit Social Media im Unternehmen widmet sich ein Beitrag auf zdnet.de: **„Social Engineering: Angriff auf Mitarbeiter-Konten“**

4 Risiko Lauschangriff

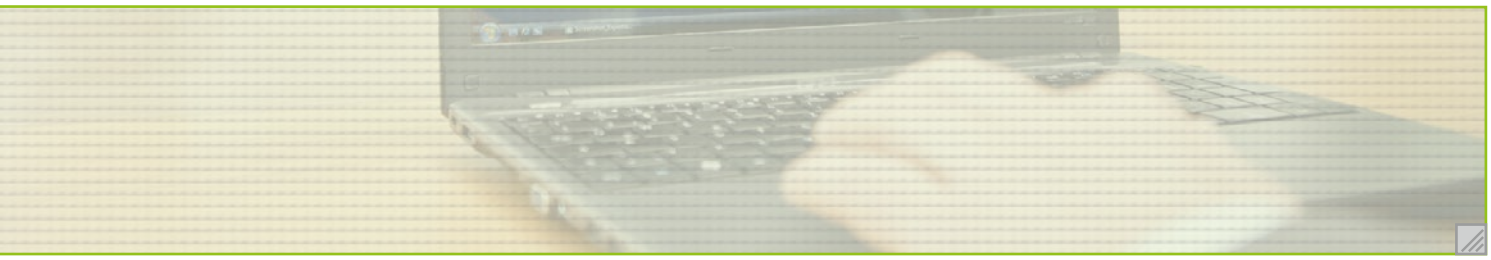
Bleiben Sie achtsam!

Freitagnachmittag: Armin ist Mitarbeiter eines mittelständischen Unternehmens. Jeden Tag pendelt er zwischen Arbeitsstätte und zu Hause – erst mit dem Bus, dann noch eine Stunde mit dem Zug. Auch heute unterhält er sich, wie es nach Feierabend üblich ist, an der Bushaltestelle noch mit seinen Kollegen über Neuigkeiten im Unternehmen – neue Mitarbeiter, geplante Umstrukturierungen, Fortschritte und vieles mehr. Und auch heute hat er sich mal wieder Arbeit mitgebracht, die er noch schnell am Firmennotebook im Zug erledigen will. Zu dumm – nach einer halben Stunde ist der Akku fast leer. Doch Armin hat ja noch sein Tablet. Schnell noch eine neue Spiele-App von einer neuen Freeware-Site heruntergeladen und schon vergeht die Zeit wie im Flug. Kurz vor seiner Ankunft prüft er noch schnell seine E-Mails und löscht störende Spam-Nachrichten, die er sofort an der ausländischen Adresse oder dem gebrochenen Deutsch erkennt.

Was macht Armin hier falsch?

Armin ist ein engagierter, offenkundig loyaler Arbeitnehmer und sogar über die Arbeitszeit hinaus an seinem Job interessiert. Dennoch bietet er Social Engineers gleich mehrere Angriffsflächen, denn er:

- a) **bespricht firmeninterne Angelegenheiten an einem öffentlichen Ort.** Das macht neugierigen Ohren das Aushorchen leicht.
- b) **ermöglicht bei der Arbeit im Zug neugierigen Blicken Einsicht in seine Arbeitsunterlagen.** Durch sogenanntes „Shoulder Surfing“ (das Über-die-Schulterblicken etwa auf den Notebook-Bildschirm oder ausgedruckte Unterlagen) gelangen nicht nur Social Engineers leicht an sensible Informationen wie z. B. Firmendaten oder Passwörter.
- c) **nutzt unsichere Download-Kanäle für Apps.** So installiert er vielleicht, ohne es zu merken, mit einer neuen App auch Malware auf seinem Tablet.
- d) **geht davon aus, dass Spam-Mails leicht zu erkennen sind.** Es gibt aber auch sehr professionelle, täuschend echt aussehende Spams in einwandfreiem Deutsch und mit gefälschter Behörden-Absenderadresse – und im Falle personalisierter Social-Engineering-Angriffe sogar solche, die extra für die Zielperson gestaltet wurden.



Gezielte Lauschangriffe

Durch das Mithören von Gesprächen oder Mitlesen von E-Mails können wichtige Informationen gesammelt werden.

Lauschangriffe finden häufig statt und sie werden immer professioneller. Die Angreifer nutzen die verschiedensten Medien und Methoden, z. B. das Mithören eines Gesprächs, das Abhören eines Telefonats oder das Mitlesen einer E-Mail. Mit den aufgefangenen Informationen können Social Engineers weit mehr anfangen, als man zunächst annehmen würde. Häufig geht es ihnen bei derartigen Lauschangriffen zunächst nur um das Kennenlernen der Unternehmensstruktur und der im Unternehmen gebräuchlichen Terminologie oder um die Namen von Personen und ihre Position im Unternehmen – alle Informationen, die beim eigentlichen Angriff von Nutzen sein können.

Der Begriff „Lauschangriff" ist also nicht allein auf das „Lauschen" beschränkt, sondern bezeichnet vielmehr generell das Sammeln von Daten, ohne dass die Opfer bewusst mit den Angreifern in Kontakt treten. Neben gezielten, persönlichen Lauschangriffen fallen darunter auch indirekte, unpersönliche Methoden, die das Internet nutzen, insbesondere die Verbreitung von Malware und Spyware sowie das „Phishing" und das „Vishing".

Lauschangriffe über das Internet

- **Verbreitung von Malware und Spyware:** Unter dem Begriff „Malware" oder auch „Evilware" fasst man verschiedene Schadprogramme zusammen, die beim Benutzer unerwünschte und zumeist schädliche Funktionen ausführen. Darunter fallen beispielsweise Viren oder Trojaner, die meist über präparierte Webseiten oder über E-Mails (meist im Anhang) verbreitet werden.

  Diese Schadprogramme sind in der Lage, den PC-Anwender umfassend auszuspionieren und etwa Tastatureingaben mitzulesen (z. B. Passwörter, Kommunikation), gezielt Dateien zu suchen und an die Angreifer zu versenden oder sogar den PC fernsteuern zu lassen.

- Zu Social-Engineering-Zwecken wird häufig auch **„Scareware"** benutzt. Dabei wird der Anwender durch Schadcode auf seinem Rechner oder beim Besuch einer bösartigen Webseite mit Meldungen verunsichert, die ihn vor angeblichen Sicherheitslücken seines PCs oder vor darauf befindlichen Viren warnen. Es gibt sogar Programme, die den PC durch Sperrung oder Verschlüsselung unbenutzbar machen, um den Benutzer zu erpressen.

  Für die Problemlösung soll der Anwender z. B. gegen Bezahlung eine Bereinigung durchführen lassen oder ein – je nach Angriffsziel kostenpflichtiges oder kostenloses – Säuberungstool installieren. Geht das Opfer darauf ein, haben die Angreifer ihr Ziel erreicht: Es geht ihnen entweder darum, schnell an Geld zu kommen (der Anwender zahlt) oder Daten abzugreifen (der Anwender installiert das Tool – meist ein getarnter Spionage-Trojaner).

- **Phishing:** Das Wort „Phishing" lehnt sich an das englische Wort für „Fishing" (= Angeln) an und bezeichnet eine Methode, bei der Angreifer versuchen, über gefälschte Webseiten oder E-Mails an Zugangsdaten (z. B. Passwörter oder Bankinformationen) zu gelangen.

  Solche Angriffe können jeden treffen: Immer wieder warnen Verbraucherzentralen, Banken und Unternehmen vor gefälschten Phishing-Mails, so z. B. im Juni 2015 vor E-Mails, die sich im Namen der „Deutschen Bank" Kundeninformationen erschleichen wollten.[9] Banken und seriöse Unternehmen betonen, dass sie vertrauliche Kundeninformationen niemals ungesichert über Telefon oder E-Mail abfragen würden.

- **Vishing:** „Vishing" ist die Kurzform für „Voice Fishing". Die Angreifer gehen nach einer ähnlichen Methode vor wie beim Phishing, nutzen jedoch kostengünstige Internet-Telefonate (Voice over IP, VoIP). Das heißt: Der Social Engineer ruft automatisiert nacheinander unzählige Telefonnummern an und erfragt unter einem Vorwand sensible Daten.

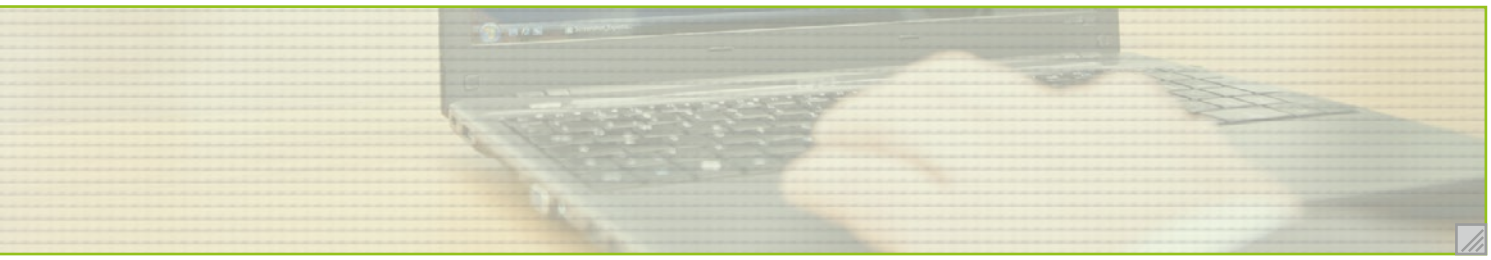
  Bei einer weiteren Vishing-Variante wird in einer E-Mail (die z. B. angeblich von der IT-Abteilung stammt), eine Telefonnummer angegeben, die die Opfer (z. B. bei PC-Problemen) anrufen sollen. Diese Methode ist besonders wirksam, da mittlerweile ein Großteil der Anwender über die Gefahrenpotenziale gefälschter Mails informiert ist und daher oftmals zuerst die hinterlegte Nummer anruft, um die Authentizität des Unternehmens zu verifizieren. Angreifer nutzen das nicht nur für das Datensammeln aus, sondern bringen häufig ihre Opfer auch dazu, unwissentlich Schadsoftware zu installieren.

- **Bitte beachten Sie:**
  Lauschangriffe finden überall statt! Ob im Büro am PC, unterwegs am mobilen Endgerät oder durch Mithören eines Gesprächs!

Risiken

1. Kriminelle verschaffen sich Zugang zu Informationen und nutzen diese zu kriminellen Handlungen (zum Beispiel Erpressung, Identitätsdiebstahl).
2. Nutzerverhalten wird beim Benutzen von Tablets oder Smartphones besonders leicht durch Malware ausgelesen.
3. Spam-Mails können täuschend echt aussehen und hochprofessionell gestaltet sein. Man kann sie heutzutage nicht mehr sicher an mangelnden Sprachkenntnissen oder ausländischen Mailadressen erkennen.

[9] www.vz-nrw.de/phishing, aktuelle Warnungen finden sich auf dem Phishing-Radar der Verbraucherzentrale Nordrhein-Westfalen



Verhaltensregeln

1. In der Öffentlichkeit sollten Sie nie über firmeninterne Angelegenheiten sprechen. Trennen Sie stets Geschäftliches von Privatem.
2. Schützen Sie Ihren Computer sowie Ihr mobiles Endgerät (z. B. Smartphone, Tablets) mit einem Virenschutz und downloaden Sie keine Software, die Ihnen als (Pop-up-)Anzeige im Internet angeboten wird.
3. Öffnen Sie keine E-Mails, deren Absender Sie nicht kennen, und denken Sie daran, dass auch Absenderadressen gefälscht werden können.
4. Geben Sie Kennwörter und Transaktionsnummern nie weiter.
5. Schützen Sie Ihre Passwörter. Vor allem Ihr E-Mail-Passwort ermöglicht es Social Engineers, Ihre Identität zu stehlen, da ein Angreifer Zugangsdaten für sämtliche Online-Dienste, bei denen Sie angemeldet sind, über die Mailadresse anfordern kann (Funktion „Passwort vergessen").
6. Benutzen Sie einen Sichtschutz für Ihr Notebook, sobald Sie in einer unsicheren Umgebung vertrauliche Firmen- bzw. private Dokumente bearbeiten.

Weiterführende Informationen und Links

- Praxisbezogene Tipps zu sicheren Passwörtern finden Sie unter **www.dsin-blog.de > Alle Themen > Passwort > Sicheres Passwort im Handumdrehen**
- Auf der IT-Security-Seite searchsecurity.de finden Sie zahlreiche Tipps und Ratschläge zu den Themen „Malware", „Mobile Security" u. v. m. Pfad: **www.searchsecurity.de > Security-Themen**
- Auf der DsiN-Webseite können Unternehmer testen, ob ihre Webseiten virenverseucht sind: **www.sicher-im-netz.de > Ratgeber&Tools > Für Unternehmen > Webseiten-Check**
- Der Artikel „Wirtschaftsspionage im Mittelstand" klärt über die Notwendigkeit von IT-Sicherheit auf. Pfad: **www.dsin-blog.de > Themen: News & Trends**

5 Risiko Telefon

Bleiben Sie achtsam!

Irina ist Unternehmerin und erhält häufig Anrufe von Firmen, die ihr Büroartikel, Technik oder Dienstleistungen verkaufen wollen. Eines Tages stellt sich ein Anrufer als IT-Techniker einer Sicherheitsfirma vor. Er teilt Irina mit, dass sich ein Trojaner auf ihrem PC befindet und er diesen gegen Bezahlung entfernen könne. Dazu müsse sie ihm nur einen temporären Remote-Zugang ermöglichen. Irina stimmt zu. Der vorgebliche Fachmann greift auf ihren PC zu, löscht auch ihr altes – nach seiner Aussage unzuverlässiges – Antivirenprogramm und installiert ein neues, „besseres" Programm. Verunsichert vom Auftreten des Anrufers, technisch klingenden Formulierungen und von den Schilderungen der Gefahren, die ihrem Unternehmen durch den gefundenen Trojaner gedroht haben sollen, gibt Irina dem angeblichen Techniker ihre Kontodaten.

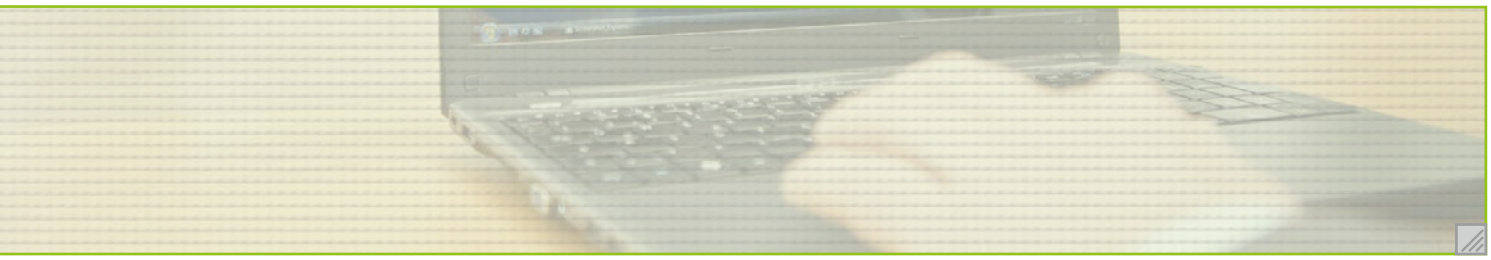
Erst als das Geld bereits eingezogen wurde und eine Rechnung ohne Absender, Adresse oder Rufnummer bei ihr eintrifft, zweifelt sie an der Vertrauenswürdigkeit des Anrufers. Doch nun ist es zu spät: Das Geld ist fort, und es ist auch nicht mehr nachvollziehbar, ob, welche und wie viele Daten bereits ausgespäht wurden. Von einem vertrauenswürdigen EDV-Dienstleister muss sie ihren PC nun neu aufsetzen lassen, um weiteren Schäden vorzubeugen.

Wie hätte Irina den Schaden verhindern können?

Es ist wichtig zu wissen, dass Social Engineers für die Kontaktaufnahme zu ihrem Opfer am liebsten zum Telefon greifen. Dieses Medium ermöglicht es ihnen, Distanz zu wahren und ihre wahre Identität zu verschleiern, aber doch flexibel auf die Reaktionen des Opfers einzugehen. Die oben beschriebene Masche ist eher plump und vielen auch bereits bekannt. Doch Social Engineers verfügen auch hier über viele unterschiedliche Methoden.

Social Engineers bauen eine persönliche Beziehung zum Opfer auf und wollen das Vertrauen gewinnen, um so an vertrauliche Informationen zu kommen.

Bei den meisten Social-Engineering-Angriffen bemerken die Opfer gar nicht, dass sie gerade einem Social Engineer wichtige Informationen weitergegeben haben. Die Stimme am Telefon klang absolut glaubwürdig: Mittels eines sogenannten „Vorangriffs" hat der Social Engineer zunächst Daten über die Unternehmensstruktur, über firmeninterne Termini (z. B. Bezeichnungen, Nummern und Abkürzungen für Abteilungen oder Prozesse) und über Personen (etwa über Facebook) gesammelt, mit denen er sich als Kollege oder langjähriger Partner ausgeben kann. Oft baut der Social Engineer eine persönliche Beziehung zum Opfer auf, indem er mehrmals anruft, sich Schritt für Schritt ein Bild aufbaut und erst nach einiger Zeit nach bestimmten Informationen fragt. Ein gewiefter Social Engineer würde auch niemals gleich auflegen, nachdem er die gewünschte Information erhalten hat. Denn der Angerufene erinnert sich später zumeist an den Anfang und das Ende des Gesprächs und nicht an einzelne, scheinbar nebensächliche Fragen, die zwischendurch gestellt wurden.



Jeder kann getäuscht werden!

Das Beispiel zeigt, dass mitunter schon ein wenig technischer Fachjargon glaubwürdig und oft auch verunsichernd wirken kann. Dies bedeutet allerdings nicht, dass nicht auch technisch versierte Mitarbeiter auf Social Engineers hereinfallen könnten. Der Angreifer hält seine Opfer nicht für dumm. Ganz im Gegenteil: Er achtet bei der Suche nach Schwachstellen ganz genau auf ihre Reaktionen, ist stets auf der Hut und tastet ab, wie weit er gehen kann. In größeren Unternehmen sind solche Angriffe noch aussichtsreicher, da sich der Social Engineer leicht als Mitarbeiter einer anderen Abteilung oder aus einem anderen Standort ausgeben kann, ohne dass der angerufene Mitarbeiter sofort Verdacht schöpft. Weil grundsätzlich jeder getäuscht werden kann, ist es besonders wichtig, vorgeschriebene Wege und Prozeduren (etwa bei technischen Problemen oder der Informationsweitergabe) einzuhalten.

- **Bitte beachten Sie:**
  Anrufer können mit falschen Angaben versuchen, an interne Informationen zu gelangen.

Risiken

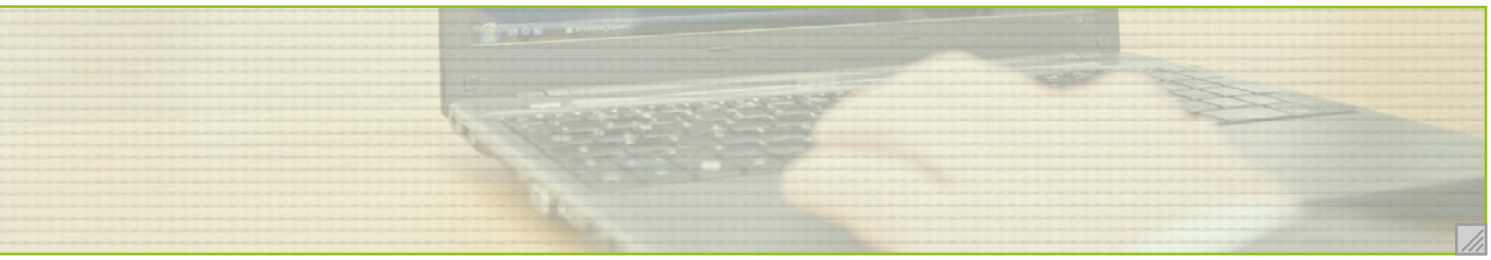
1. Social Engineers sind Meister der Täuschung und wissen, wie man sich Vertrauen verschafft. Die meisten Opfer bemerken den Angriff nicht einmal.
2. „Vorangriff“: Daten und Informationen, die Sie als unwichtig empfinden, können dem Social Engineer bereits viel über das Unternehmen verraten. Durch Vorangriffe eignet er sich Wissen und Fachjargon an, um authentisch und glaubwürdig zu wirken.
3. Wenn Sie Anrufern Zugriff auf Ihren PC geben, können diese Malware installieren, Daten stehlen oder sogar den Rechner lahmlegen und Sie erpressen.

Verhaltensweisen

1. Seien Sie unerwarteten Anrufen gegenüber stets skeptisch.
2. Überprüfen Sie die Identität des unbekannten Anrufers. Bereits detaillierte Nachfragen zur Abteilung und seinem Ansinnen können den Anrufer irritieren.
3. Holen Sie sich eine zweite Meinung ein, wenn Sie sich über ein computertechnisches Thema im Unklaren sind oder wenn Sie nicht wissen, wie vertraulich eine Information wirklich ist.

Weiterführende Informationen und Links

- Das **IT-Finanzmagazin** berichtet am 8. April 2015 über einen kombinierten Angriff per Trojaner und Telefon: **„Social Engineering: Angebliche Bank-Callcenter machen Dyre-Wolf Trojaner hochgefährlich"**
- Ein weiteres Beispiel aus der Realität lesen Sie unter **www.dsin-blog.de > Themen > Awareness > „Achtung Betrüger"**
- Ein reales Beispiel für die Social-Engineering-Methode, mit der im Beispiel Irina getäuscht wurde, beschreibt heise.de am 19. Juni 2015 im Artikel **„Betrugsmasche aufgewärmt: Falsche Microsoft-Techniker am Telefon"**



6 Risiko USB-Stick

Ali ist Mitarbeiter einer mittelgroßen Steuerkanzlei. Da er täglich mit sensiblen Informationen seiner Klienten umgeht, achtet er sehr genau auf den Datenschutz und prüft Dokumente, die er weitergibt, stets mehrfach auf die Einhaltung aller Vorschriften. Als er eines Tages im Flur der Kanzlei einen USB-Stick auf dem Boden findet, steckt er diesen sicherheitshalber zuerst in sein Arbeitsnotebook, um zu überprüfen, dass sich keine vertraulichen Daten auf dem Stick befinden, bevor er diesen beim IT-Beauftragten abgibt.

Bleiben Sie achtsam!

Welche möglichen Gefahren birgt Alis Handeln?

Auch bei gefundener Hardware muss man unbedingt Vorsicht walten lassen! Denn auf USB-Sticks kann sich Malware in Form von Viren oder Trojanern befinden. Viele ältere PCs (vor Windows 7) installieren diese unter Umständen sogar automatisch ohne Zutun des Anwenders. Außerdem ist es heute sogar technisch möglich, die Firmware von USB-Sticks so zu verändern, dass sie sich gegenüber dem Betriebssystem zum Beispiel als Tastatur oder Netzwerkkarte ausgeben. Solche Sticks könnten einen Rechner umfassend ausspionieren.

Fremde USB-Sticks sollten keinesfalls verwendet werden.

Ein Social Engineer deponiert manipulierte USB-Sticks im Unternehmen oder verteilt sie beispielsweise kostenlos auf Messen oder an Werbeständen in der Stadt. Nun muss er nur noch abwarten, bis der Stick an einen PC angeschlossen wird. Je nach Schadprogramm kann er dann auf dem Rechner gespeicherte Daten auslesen oder sogar per Remote-Zugang auf den PC zugreifen.

- **Bitte beachten Sie:**
  Fremde USB-Sticks bieten Kriminellen eine Möglichkeit, Ihre Daten auszulesen oder sogar Ihren PC fernzusteuern!

Risiken

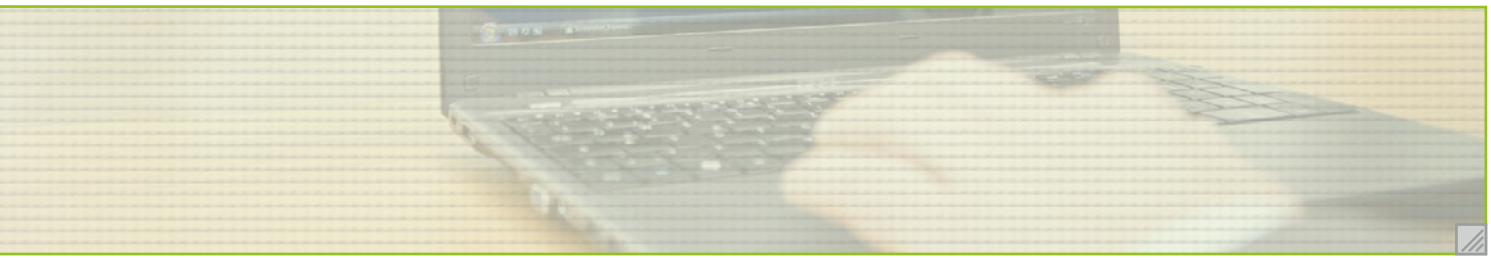
1. Gefundene oder verschenkte USB-Sticks könnten Malware beinhalten und beim Einstecken Ihren PC infiltrieren.
2. Durch die installierten Schadprogramme können die Angreifer Ihre Daten auslesen, ohne dass Sie es merken.
3. Auf dem Stick gespeicherte Viren können unter Umständen Ihren PC fernsteuern oder auch das komplette Netzwerk lahmlegen.

Verhaltensweisen

1. Verzichten Sie auf USB-Sticks, wenn Sie Ihnen als Werbegeschenk angeboten werden – auch wenn Sie sie sehr nützlich finden. USB-Sticks können heute sehr günstig im Elektronikgeschäft erworben werden.
2. Stecken Sie gefundene oder von Unbekannten geschenkte USB-Sticks NIEMALS an Ihren privaten oder betrieblichen Computer.
3. Sollten Sie USB-Sticks im Unternehmen finden, geben Sie diese, entsprechend der Unternehmensrichtlinien beim Sicherheitsdienst bzw. Ihrer Führungskraft ab oder zerstören Sie diesen umgehend.

Weiterführende Informationen und Links

- Nützliche Artikel finden Sie unter: **www.it-sicherheit.de > Ratgeber > IT-Sicherheitstipps > Basisschutz für Ihren PC > „Sicherer Umgang mit Wechseldatenträgern“** sowie **www.it-sicherheit.de > Ratgeber > IT-Sicherheitstipps > Sicherheit für Unternehmen > „Sicherheitstipp: Wirtschaftsspionage per USB-Stick“**



7 Risiko Innentäter

Marcel arbeitet bei einem mittelständischen Unternehmen. Zu seinen täglichen Aufgaben gehören unter anderem das Erfassen von Kundeninformationen und ihr Einpflegen in das Firmensystem. Viele seiner Kollegen kennt er persönlich, andere nur vom Namen, denn das Unternehmen verfügt über mehrere Abteilungen. In der Kantine lernt er Gina kennen. Sie trägt zwar keinen Mitarbeiterausweis, aber erzählt Marcel, dass sie erst seit Kurzem im Unternehmen arbeitet und zur Abteilung „Sicherheitsmanagement" gehört. Im Gespräch entdecken die beiden, dass sie recht ähnliche Aufgabengebiete haben. Einige Tage später ruft Gina in Marcels Büro an, um ihn um Hilfe zu bitten, da sie sich mit einigen Abläufen noch schwertut. Erfreut über ihr Vertrauen, gibt Marcel gerne Starthilfe und leitet Gina wichtige Kundeninformationen weiter, die sie zur Bearbeitung benötigt.

Bleiben Sie achtsam!

Wieso müsste Marcel hier vorsichtig sein?

Jeder möchte an seinem Arbeitsplatz und im Unternehmen ein angenehmes Klima schaffen und Kollegen bei Fragen behilflich sein. Doch wie kann Marcel sich sicher sein, ob der angebliche Neuling auch wirklich im Unternehmen arbeitet – und wenn ja, ob er auch befugt ist, vertrauliche Kundendaten zu bearbeiten? Doch selbst ein Mitarbeiter hat nicht automatisch das Recht, sensible Informationen aus anderen Abteilungen zu erhalten. Marcel hätte daher Gina keine vertraulichen Daten geben dürfen, denn:

- a) er kennt keine Kollegen, die bei dem Treffen anwesend waren und Ginas Stellung im Unternehmen bestätigen können.
- b) Marcel kennt Ginas Aufgabe im Unternehmen nur durch ihre Erzählungen. Er kann deshalb nicht sicher davon ausgehen, dass sie autorisiert ist, Zugriff auf die angefragten Informationen zu erhalten.
- c) im Unternehmen gibt es zwar überwachte Eingänge, doch es kann nicht ausgeschlossen werden, dass sich ein Social Engineer Zutritt in die Firma verschafft.

Social Engineers als Innentäter

Man kann zwischen zwei Kategorien von Innentätern unterscheiden:

- 1. Der Social Engineer ist kein Mitarbeiter des Unternehmens. Er hat sich unbefugt Zutritt verschafft oder gibt sich am Telefon bzw. per E-Mail als Mitarbeiter aus.
- 2. Der Social Engineer ist tatsächlich Mitarbeiter der Firma, hat aber kriminelle Intentionen. Möglicherweise
  - a) möchte er an firmeninterne Daten gelangen, um sie an die Konkurrenz zu verkaufen oder sie für persönliche Zwecke zu nutzen (eigenständige Entwicklung, geldwerte Vorteile).
  - b) ist er bereits bei einem anderen Unternehmen angestellt und betreibt Unternehmensspionage.

Social-Engineer-Angreifer können neben externen Personen auch Mitarbeiter aus dem eigenen Unternehmen sein.

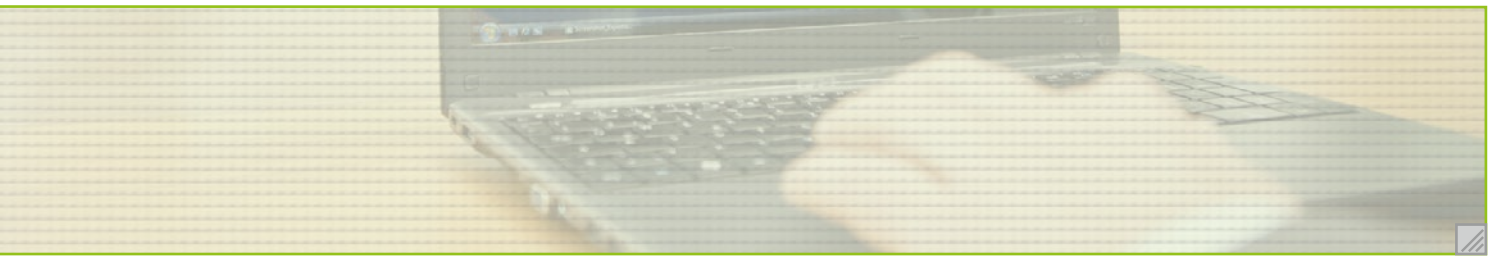
Die meisten erfolgreichen Angriffe auf ein Unternehmen erfolgen aus den inneren Reihen! Nach der oben zitierten Bitkom-Studie[1] treten bei mehr als der Hälfte (51 %) der Fälle von Spionage, Datendiebstahl oder Sabotage in Unternehmen aktuelle oder ehemalige Mitarbeiter als Täter in Erscheinung. Diese Täter benötigen meist viel weniger Aufwand, um an Informationen zu gelangen, denn sie kennen nicht nur Abläufe und Sicherheitsvorkehrungen, sondern wissen auch, an wen sie sich wenden müssen und wie sie Vertrauen herstellen können.

Die häufigsten Angriffe von Innentätern finden über das Telefon statt. Besonders bei großen Firmen ist die Wahrscheinlichkeit groß, dass sich nicht alle Mitarbeiter untereinander kennen. Mitarbeiter größerer Unternehmen können deshalb in Bezug auf Firmenzugehörigkeit oder Kompetenzen leicht getäuscht werden. Im Beispiel oben hat sich die Angreiferin so erst das Vertrauen des Angestellten erschlichen und dann seine Gutmütigkeit und Hilfsbereitschaft ausgenutzt.

- **Bitte beachten Sie:**
  Sensible Daten dürfen selbst unter Kollegen nur an autorisierte Personen weitergegeben werden!

Risiken

1. Durch „zufällige" Treffen in der Mittagspause oder beim Kaffeetrinken können sich Innentäter das Vertrauen eines Kollegen leicht erschleichen.
2. Die Gefahr, unberechtigt sensible Informationen weiterzugeben, ist durch die vermeintliche Vertrauensbasis unter Kollegen sehr hoch.
3. Auch bei entsprechenden Sicherheitsvorkehrungen besteht das Risiko, dass sich ein Täter nur als Mitarbeiter der Firma ausgibt und sich unbefugt Zutritt verschafft hat.



Verhaltensregeln

- 1. Überprüfen Sie wenn möglich die Identität und Autorisation des Kollegen.
- 2. Melden Sie auffälliges Verhalten Ihrer Führungskraft oder sprechen Sie die Person direkt an (zum Beispiel, wenn ein Mitarbeiter keinen Ausweis trägt, obwohl es im Unternehmen vorgeschrieben ist).
- 3. Unterstützen Sie Ihre Mitarbeiter, sich auch in Notsituationen an die vereinbarten Vorgehensweisen zur Autorisation zu halten. Sicherheitspersonal sollte spezielle Schulungen zu diesem Thema erhalten (z. B. Zutrittskontrolle).

Weiterführende Informationen und Links

- Der Verfassungsschutz bietet auf seiner Webseite ein Faltblatt zum Thema an: **www.verfassungsschutz.de > Öffentlichkeitsarbeit > Publikationen > Geheim-, Sabotage- und Wirtschaftsschutz > Faltblatt „Sicherheitslücke Mensch – Der Innentäter als größte Bedrohung für die Unternehmen“**
- **Interessieren Sie sich für weitere (reale) Beispiele und Methoden?** In seinem Buch **„Die Kunst der Täuschung: Risikofaktor Mensch“** beschreibt Kevin Mitnick die Techniken eines Social Engineers ausführlich aus eigener Erfahrung. Um Innentäter (der 1. Kategorie) geht es v. a. in Teil 3.

8 Trau, schau, wem – Bleiben Sie achtsam!

Social Engineering nutzt gezielt ganz normale menschliche Eigenschaften aus – Hilfsbereitschaft, Gutgläubigkeit und vor allem das grundlegende Vertrauen zu anderen Personen. Deshalb schützen uns vor solchen Angriffen keine Firewalls oder andere technischen Maßnahmen. Es gibt nur einen einzigen wirksamen Schutz vor Social Engineering: ein gesundes Misstrauen, verbunden mit dem strikten Einhalten vereinbarter Regeln zur Datenweitergabe!

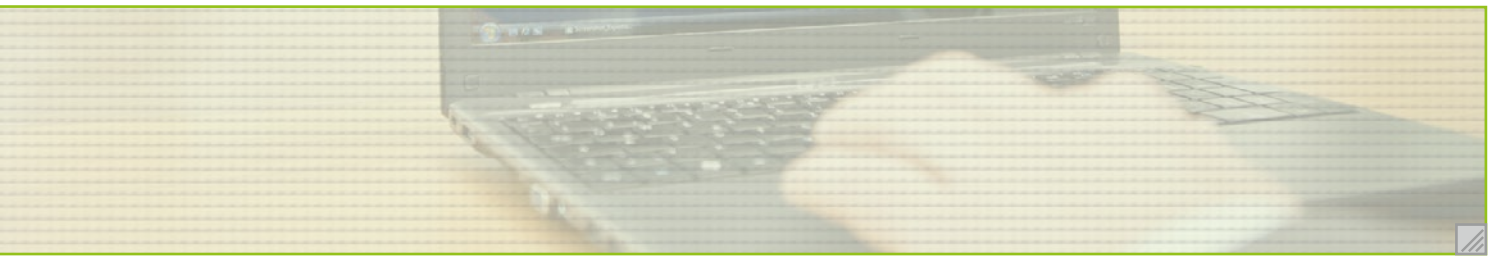
Gesundes Misstrauen

Jetzt, da Sie die Methoden und Tricks der Social Engineers besser kennen, wird es Ihnen leichter fallen, fremden Personen und auch flüchtigen Bekannten gegenüber skeptisch zu bleiben. Wie aber sieht es mit gut bekannten Kollegen aus, mit denen Sie eng zusammenarbeiten? Das kollegiale Vertrauensverhältnis ist sehr wichtig für eine entspannte und produktive Arbeitsatmosphäre. „Gesundes" Misstrauen meint eine Grundeinstellung, die dieses Vertrauensverhältnis nicht gefährdet. Wie aber ist das möglich?

Sie wissen, dass ein Social-Engineering-Angriff jeden treffen kann und dass jeder Mensch auch erfolgreich getäuscht werden kann. Davor ist niemand von uns gefeit. Deshalb können selbst absolut vertrauenswürdige Kollegen womöglich dazu gebracht werden, Sie um Informationen zu bitten, die Sie nicht herausgeben sollten. Wenn Ihnen eine solche Bitte ungewöhnlich vorkommt, fragen Sie nach, lassen Sie sich das Problem erklären, ziehen Sie bei Bedarf Ihre Führungskraft hinzu – aber handeln Sie nicht gegen die Regeln!

Regeln strikt einhalten

Regeln haben eine nützliche Eigenschaft: In passenden Situationen ersparen sie uns Entscheidungen, indem sie die richtige Handlung vorgeben. Nutzen Sie das aus! Sobald es um sensible Daten geht – und das sind nicht nur Zugangsdaten oder vertrauliche Informationen, sondern auch alle Arten von Firmeninterna (Strukturen, Prozesse) und von personengebundenen Daten (Namen, Funktionen, Telefonnummern etc.) – müssen entsprechende Regeln in der Firma strikt eingehalten werden. Wenn Sie regelwidrige Auskünfte stets freundlich ablehnen oder auf den vorgeschriebenen Dienstweg verweisen, dann handeln Sie nicht etwa unkooperativ, sondern helfen Ihrer Firma und Ihren Kollegen dabei, weiterhin vertrauensvoll zusammenzuarbeiten.



Die eigene Anfälligkeit kennen

Vor allem aber sollten Sie das „gesunde Misstrauen“ auf sich selbst richten: Fühlen Sie sich nicht zu sicher! Denken Sie daran, dass jeder gefährdet ist, unabhängig von Position und Kenntnissen. Sie sind für Ihr Unternehmen eventuell wichtiger, als Sie selbst es glauben, und mit Sicherheit verfügen Sie über sehr vertrauliche Informationen, die Social Engineers interessieren könnten – von den Geburtstagen und Hobbys Ihrer Kollegen über Abteilungsbezeichnungen bis hin zu neu geplanten Produktfunktionen.

Deshalb sollten Sie sich stets auch Ihrer ganz persönlichen Angriffsflächen für Social Engineers bewusst sein, die von Arbeits- und Kommunikationsgewohnheiten und den Umgang mit sozialen Netzwerken bis hin zum Grad der eigenen Gutgläubigkeit und Vertrauensbereitschaft reichen. Der Fragebogen im Anhang kann Ihnen dabei helfen.

Getreu dem Motto:
Gesundes Misstrauen lohnt sich! Jeden Tag!

9 Anhang: Wie vorsichtig bin ich?

Selbstkontrolle

1.

In der Firma ruft Sie ein Kollege aus dem Rechnungswesen an und fragt Sie nach Ihren persönlichen Daten ([E-Mail-]Adresse, Kontodaten), da zukünftig die Lohnabrechnungen nach Hause geschickt werden sollen.

A Obwohl die Stimme mir bekannt vorkommt und der Kollege sich bereits ärgert, prüfe ich die Identität anhand der angezeigten Daten am Telefon.

B Wenn ich den Kollegen an der Stimme erkenne, gebe ich die Daten weiter.

C Da meine Adresse dem Unternehmen ohnehin bekannt ist, besteht hier keine Gefahr. Ich gebe sie zur Erleichterung des Verfahrens durch.

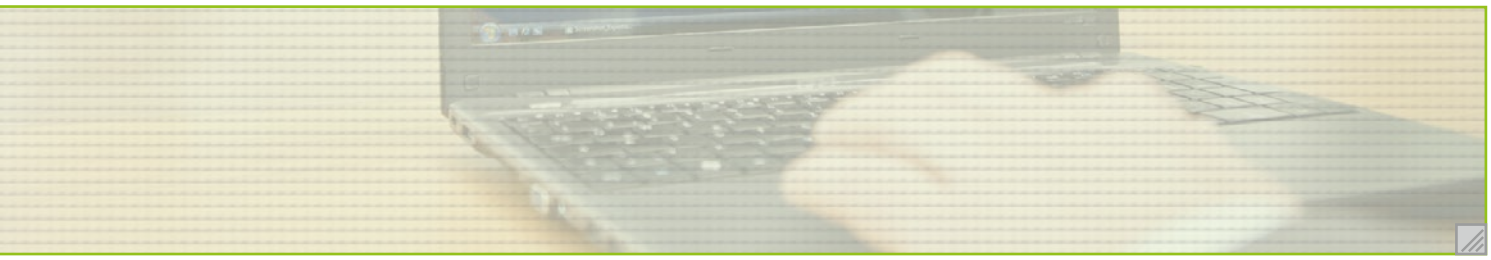
2.

Sie erhalten immer wieder Spam-Mails und erkennen diese an der falschen Rechtschreibung oder dem mysteriösen Absender. Unter anderem erhalten Sie aber auch sehr gut gefälschte E-Mails.
Wie gehen Sie damit um?

A Ich bin schon einmal auf eine gefälschte Mail hereingefallen und habe geantwortet. Seither bin ich sehr skeptisch, was E-Mails betrifft.

B Ich habe bereits öfter gut gemachte Spam-Mails erhalten und frage seitdem immer erst bei mir persönlich bekannten Ansprechpartnern nach, ob die Mail wirklich von dem Unternehmen/der Bank stammt.

C Leider falle ich immer wieder auf diese Mails herein. Mittlerweile sind sie so gut gemacht, dass ich sie einfach nicht von seriösen Mails unterscheiden kann. Wenn ich mir nicht sicher bin, öffne ich sie oft, um sicherzugehen, dass wirklich nichts Wichtiges darin steht.



3.

Ein Kollege, den Sie nur über das Telefon kennen, ruft sehr häufig an, um Ihrer Meinung nach eher unwichtige Fragen zu stellen. Dieses Verhalten kommt Ihnen seltsam vor, jedoch geben Sie dabei nur unwichtige Informationen weiter. Wie verhalten Sie sich?

A Sie informieren sich selbst über den angeblichen Kollegen und ignorieren weitere Anrufe, wenn sich herausstellt, dass dieser nicht zum Unternehmen gehört.

B Sie informieren Ihre Führungskraft bei der nächsten Gelegenheit, damit diese entsprechend handelt.

C Ihrer Führungskraft erzählen Sie davon erst etwas, wenn der Anrufer spezifischere Fragen stellt. Sie wissen, dass ihre Führungskraft darauf vertraut, dass Sie zwischen lästigen Nachfragen und echten Bedrohungen unterscheiden können.

4.

Auf dem Weg zur Arbeit oder nach Feierabend unterhalten Sie sich mit Kollegen, arbeiten oft noch am Notebook oder Tablet weiter oder nutzen das Smartphone für Firmenmails und -anrufe. Worauf achten Sie?

A Darauf, dass ich möglichst alleine bin und so niemand meine Gespräche mithören kann oder Einblick in meine Unterlagen erhält.

B Ich habe noch nie die Erfahrung gemacht, dass irgendjemand an meinem Berufsleben interessiert wäre. Also muss ich hier auch keine Vorsichtsmaßnahmen ergreifen.

C Ich benutze für mein Notebook immer einen Sichtschutz. An öffentlichen Orten rede ich nie über Firmeninterna, auch nicht mit Kollegen.

5.

Wie verhalten Sie sich in sozialen Netzwerken?

A Ich bin ein sehr kommunikativer und vernetzter Mensch. Viele Freunde im Netz zu haben und mit ihnen Inhalte zu teilen, ist mir wichtig, und da ich nichts teile, das mit der Firma in Verbindung steht, sehe ich da auch kein Problem.

B Da ich nur Personen in meine Freundesliste aufnehme, die ich wirklich kenne, teile ich gerne alles mit ihnen. Ich kann mir ja sicher sein, dass nur die richtigen Personen meine Inhalte sehen.

C Ich versuche, meine Privatsphäre-Einstellungen immer zu aktualisieren und achte darauf, wer in meiner Freundesliste ist. Zwar schaffe ich das nicht sehr regelmäßig, wenn es allerdings Neuerungen gibt, kümmere ich mich sofort darum.

6.

Sie bemerken zwei Personen, die sich angeregt unterhalten und ohne Firmenausweis durch den Gang schlendern. Sie weisen die beiden darauf hin, dass sie keinen Ausweis tragen. Daraufhin antworten die beiden: „Den lassen wir eigentlich immer im Büro. Wir gehören zur Abteilung XY." Einige Tage später sehen Sie eine der Personen erneut ohne Firmenausweis. Was tun Sie?

A Sie sprechen die Person noch einmal freundlich auf das Fehlen des Ausweises an und fragen erneut nach Namen und Abteilung. Sie begleiten den „Kollegen" zum Sicherheitsdienst oder zu Ihrer Führungskraft, sollte dieser sich diesmal nicht ausweisen können.

B Sie sprechen die Person nicht an, denn Sie wissen nach dem letzten Gespräch, zu welcher Abteilung sie gehört.

C Sie sprechen die Person erneut darauf an und belassen es dabei.

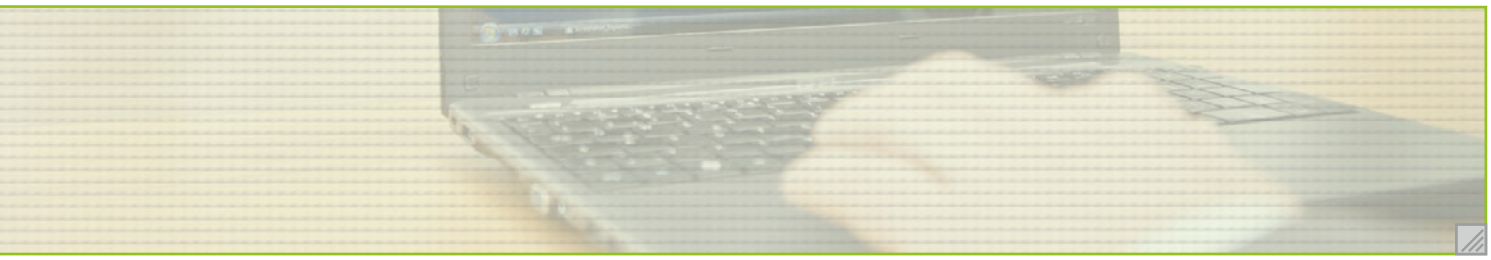
7.

An einem Werbestand werden USB-Sticks verschenkt.
Wie reagieren Sie?

A Sie nehmen den Stick gerne an, überprüfen ihn aber zunächst am Firmen-PC mit einem Virenschutzprogramm.

B Sie nehmen den Stick gerne an und überprüfen ihn zu Hause mit einem Virenscanner.

C Sie lehnen das Geschenk ab, da Sie die damit einhergehenden Gefahren kennen, und kaufen sich bei Bedarf selbst einen USB-Stick.



Punkteverteilung

	Antwort A	Antwort B	Antwort C
Frage 1	**2**	**1**	**0**
Frage 2	**1**	**2**	**0**
Frage 3	**0**	**2**	**1**
Frage 4	**1**	**0**	**2**
Frage 5	**0**	**1**	**2**
Frage 6	**2**	**0**	**1**
Frage 7	**0**	**1**	**2**
Gesamt			

Falsche Antwort	**0 Punkte**
Zweitbeste Antwort	**1 Punkt**
Beste Antwort	**2 Punkte**

Auswertung

0–6 Punkte Amateur

Sie möchten nicht negativ auffallen, weil Sie Ihrer Führungskraft alles melden und gegenüber jedem höflich und hilfsbereit sind. Das sind sympathische Eigenschaften, doch sie schützen leider nicht vor Social Engineering! Seien Sie in Zukunft skeptischer und hinterfragen Sie mehr. Dieser Leitfaden kann Ihnen dabei helfen.

7–11 Punkte Fortgeschrittener

Sie sind auf dem richtigen Weg und haben schon eine gewisse Skepsis entwickelt. Orientieren Sie sich an dem Kalender und hinterfragen Sie gewisse Situationen noch genauer. Weiter so!

12–14 Punkte Experte

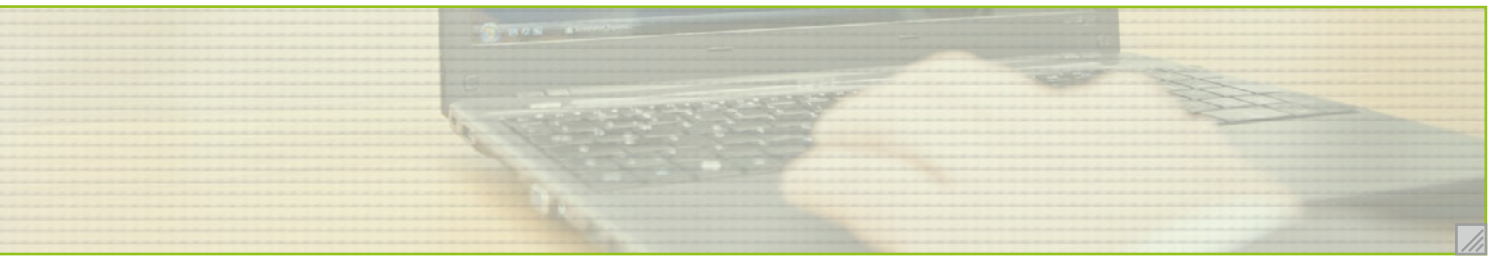
Sie haben ein gesundes Misstrauen und wissen mit möglichen Angreifern umzugehen. Herzlichen Glückwunsch! Die Devise lautet weiterhin: Gesundes Misstrauen lohnt sich. Jeden Tag!

Weiterführende Informationen und Links:
Unter nachfolgendem Link finden Sie diesen Leitfaden auch als PDF zum Download: www.datev.de/sicherheitsleitfaden

10 Erinnerungs-Karte zum downloaden

Damit Sie nachhaltig achtsam bleiben und die größten Risiken des Social Engineering immer im Blick haben, einfach die Karte hier downloaden und ausdrucken.

↗ **www.datev.de/sicherheitsleitfaden > Leitfaden „Verhaltensregeln zum Thema Social Engineering“**



Herausgeber:
Deutschland sicher im Netz e.V.
Albrechtstraße 10a
10117 Berlin
info@sicher-im-netz.de
www.sicher-im-netz.de

Art.-Nr. 16258 2015-09-01 1. Auflage